aws

參考指南

AWS 受管政策

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 受管政策: 參考指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS 受管政策？ 1
了解政策參考頁面 1
已棄用 AWS 受管政策 2
AWS 受管政策 3
AccessAnalyzerServiceRolePolicy 52
使用此政策 52
政策詳細資訊 52
政策版本 52
JSON 政策文件 53
進一步了解 55
AccountManagementFromVercel 55
使用此政策 55
政策詳細資訊 56
政策版本 56
JSON 政策文件 56
進一步了解 57
AdministratorAccess 57
使用此政策 57
政策詳細資訊 57
政策版本 57
JSON 政策文件 58
進一步了解 58
AdministratorAccess-Amplify 58
使用此政策 58
政策詳細資訊 58
政策版本 59
JSON 政策文件 59
進一步了解 69
AdministratorAccess-AWSElasticBeanstalk 69
使用此政策 69
政策詳細資訊 70
政策版本 70
JSON 政策文件 70
進一步了解 78

AIOpsAssistantIncidentReportPolicy 78
使用此政策 78
政策詳細資訊 79
政策版本 79
JSON 政策文件 79
進一步了解 80
AIOpsAssistantPolicy 80
使用此政策 80
政策詳細資訊 80
政策版本 80
JSON 政策文件 81
進一步了解 101
AIOpsConsoleAdminPolicy 102
使用此政策 102
政策詳細資訊 102
政策版本 102
JSON 政策文件 102
進一步了解 108
AIOpsOperatorAccess 108
使用此政策 109
政策詳細資訊 109
政策版本 109
JSON 政策文件 109
進一步了解 112
AIOpsReadOnlyAccess 112
使用此政策 112
政策詳細資訊 112
政策版本 113
JSON 政策文件 113
進一步了解 113
AlexaForBusinessDeviceSetup 114
使用此政策 114
政策詳細資訊 114
政策版本 114
JSON 政策文件 114
進一步了解 115

AlexaForBusinessFullAccess 115
使用此政策 115
政策詳細資訊 115
政策版本 116
JSON 政策文件 116
進一步了解 117
AlexaForBusinessGatewayExecution 117
使用此政策 117
政策詳細資訊 118
政策版本 118
JSON 政策文件 118
進一步了解 119
AlexaForBusinessLifesizeDelegatedAccessPolicy 119
使用此政策 119
政策詳細資訊 119
政策版本 120
JSON 政策文件 120
進一步了解 122
AlexaForBusinessNetworkProfileServicePolicy 122
使用此政策 122
政策詳細資訊 122
政策版本 123
JSON 政策文件 123
進一步了解 124
AlexaForBusinessPolyDelegatedAccessPolicy 124
使用此政策 124
政策詳細資訊 124
政策版本 124
JSON 政策文件 124
進一步了解 126
AlexaForBusinessReadOnlyAccess 126
使用此政策 126
政策詳細資訊 127
政策版本 127
JSON 政策文件 127
進一步了解 127

AmazonAPIGatewayAdministrator 128
使用此政策 128
政策詳細資訊 128
政策版本 128
JSON 政策文件 128
進一步了解 129
AmazonAPIGatewayInvokeFullAccess 129
使用此政策 129
政策詳細資訊 129
政策版本 129
JSON 政策文件 129
進一步了解 130
AmazonAPIGatewayPushToCloudWatchLogs 130
使用此政策 130
政策詳細資訊 130
政策版本 131
JSON 政策文件 131
進一步了解 131
AmazonAppFlowFullAccess 131
使用此政策 132
政策詳細資訊 132
政策版本 132
JSON 政策文件 132
進一步了解 135
AmazonAppFlowReadOnlyAccess 135
使用此政策 135
政策詳細資訊 135
政策版本 135
JSON 政策文件 136
進一步了解 136
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy 136
使用此政策 137
政策詳細資訊 137
政策版本 137
JSON 政策文件 137
進一步了解 138

AmazonAppStreamFullAccess 138
使用此政策 138
政策詳細資訊 138
政策版本 139
JSON 政策文件 139
進一步了解 141
AmazonAppStreamPCAAccess 141
使用此政策 141
政策詳細資訊 141
政策版本 141
JSON 政策文件 141
進一步了解 142
AmazonAppStreamReadOnlyAccess 142
使用此政策 142
政策詳細資訊 142
政策版本 143
JSON 政策文件 143
進一步了解 143
AmazonAppStreamServiceAccess 143
使用此政策 143
政策詳細資訊 144
政策版本 144
JSON 政策文件 144
進一步了解 145
AmazonAthenaFullAccess 145
使用此政策 145
政策詳細資訊 146
政策版本 146
JSON 政策文件 146
進一步了解 149
AmazonAthenaServiceRolePolicy 150
使用此政策 150
政策詳細資訊 150
政策版本 150
JSON 政策文件 150
進一步了解 151

AmazonAugmentedAIFullAccess 151
使用此政策 151
政策詳細資訊 151
政策版本 151
JSON 政策文件 152
進一步了解 153
AmazonAugmentedAIHumanLoopFullAccess 153
使用此政策 153
政策詳細資訊 153
政策版本 153
JSON 政策文件 153
進一步了解 154
AmazonAugmentedAIIntegratedAPIAccess 154
使用此政策 154
政策詳細資訊 154
政策版本 155
JSON 政策文件 155
進一步了解 156
AmazonAuroraDSQLConsoleFullAccess 156
使用此政策 156
政策詳細資訊 156
政策版本 157
JSON 政策文件 157
進一步了解 159
AmazonAuroraDSQLFullAccess 159
使用此政策 159
政策詳細資訊 159
政策版本 160
JSON 政策文件 160
進一步了解 162
AmazonAuroraDSQLReadOnlyAccess 162
使用此政策 162
政策詳細資訊 162
政策版本 163
JSON 政策文件 163
進一步了解 163

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy 164
使用此政策 164
政策詳細資訊 164
政策版本 164
JSON 政策文件 164
進一步了解 165
AmazonBedrockFullAccess 165
使用此政策 165
政策詳細資訊 165
政策版本 166
JSON 政策文件 166
進一步了解 171
AmazonBedrockLimitedAccess 171
使用此政策 171
政策詳細資訊 171
政策版本 172
JSON 政策文件 172
進一步了解 174
AmazonBedrockMantleFullAccess 174
使用此政策 174
政策詳細資訊 174
政策版本 174
JSON 政策文件 175
進一步了解 175
AmazonBedrockMantleInferenceAccess 175
使用此政策 175
政策詳細資訊 175
政策版本 176
JSON 政策文件 176
進一步了解 176
AmazonBedrockMantleReadOnly 177
使用此政策 177
政策詳細資訊 177
政策版本 177
JSON 政策文件 177
進一步了解 178

AmazonBedrockMarketplaceAccess 178
使用此政策 178
政策詳細資訊 178
政策版本 179
JSON 政策文件 179
進一步了解 183
AmazonBedrockReadOnly 183
使用此政策 183
政策詳細資訊 183
政策版本 184
JSON 政策文件 184
進一步了解 185
AmazonBedrockStudioPermissionsBoundary 185
使用此政策 186
政策詳細資訊 186
政策版本 186
JSON 政策文件 186
進一步了解 190
AmazonBraketFullAccess 190
使用此政策 190
政策詳細資訊 191
政策版本 191
JSON 政策文件 191
進一步了解 195
AmazonBraketJobsExecutionPolicy 195
使用此政策 196
政策詳細資訊 196
政策版本 196
JSON 政策文件 196
進一步了解 199
AmazonBraketServiceRolePolicy 199
使用此政策 199
政策詳細資訊 199
政策版本 199
JSON 政策文件 199
進一步了解 200

AmazonChimeFullAccess 200
使用此政策 201
政策詳細資訊 201
政策版本 201
JSON 政策文件 201
進一步了解 203
AmazonChimeReadOnly 203
使用此政策 203
政策詳細資訊 204
政策版本 204
JSON 政策文件 204
進一步了解 204
AmazonChimeSDK 205
使用此政策 205
政策詳細資訊 205
政策版本 205
JSON 政策文件 205
進一步了解 206
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 206
使用此政策 207
政策詳細資訊 207
政策版本 207
JSON 政策文件 207
進一步了解 208
AmazonChimeSDKMessagingServiceRolePolicy 208
使用此政策 209
政策詳細資訊 209
政策版本 209
JSON 政策文件 209
進一步了解 210
AmazonChimeServiceRolePolicy 210
使用此政策 210
政策詳細資訊 210
政策版本 210
JSON 政策文件 211
進一步了解 211

AmazonChimeTranscriptionServiceLinkedRolePolicy 211
使用此政策 211
政策詳細資訊 212
政策版本 212
JSON 政策文件 212
進一步了解 212
AmazonChimeUserManagement 213
使用此政策 213
政策詳細資訊 213
政策版本 213
JSON 政策文件 213
進一步了解 214
AmazonChimeVoiceConnectorServiceLinkedRolePolicy 215
使用此政策 215
政策詳細資訊 215
政策版本 215
JSON 政策文件 215
進一步了解 217
AmazonCloudDirectoryFullAccess 217
使用此政策 217
政策詳細資訊 217
政策版本 218
JSON 政策文件 218
進一步了解 218
AmazonCloudDirectoryReadOnlyAccess 218
使用此政策 218
政策詳細資訊 219
政策版本 219
JSON 政策文件 219
進一步了解 219
AmazonCloudWatchEvidentlyFullAccess 220
使用此政策 220
政策詳細資訊 220
政策版本 220
JSON 政策文件 220
進一步了解 223

AmazonCloudWatchEvidentlyReadOnlyAccess 223
使用此政策 223
政策詳細資訊 223
政策版本 223
JSON 政策文件 224
進一步了解 224
AmazonCloudWatchEvidentlyServiceRolePolicy 224
使用此政策 224
政策詳細資訊 225
政策版本 225
JSON 政策文件 225
進一步了解 226
AmazonCloudWatchRUMFullAccess 227
使用此政策 227
政策詳細資訊 227
政策版本 227
JSON 政策文件 227
進一步了解 230
AmazonCloudWatchRUMReadOnlyAccess 230
使用此政策 230
政策詳細資訊 230
政策版本 230
JSON 政策文件 230
進一步了解 232
AmazonCloudWatchRUMServiceRolePolicy 232
使用此政策 232
政策詳細資訊 232
政策版本 232
JSON 政策文件 233
進一步了解 233
AmazonCodeCatalystFullAccess 233
使用此政策 234
政策詳細資訊 234
政策版本 234
JSON 政策文件 234
進一步了解 235

AmazonCodeCatalystReadOnlyAccess 235
使用此政策 235
政策詳細資訊 235
政策版本 236
JSON 政策文件 236
進一步了解 236
AmazonCodeCatalystSupportAccess 236
使用此政策 236
政策詳細資訊 237
政策版本 237
JSON 政策文件 237
進一步了解 238
AmazonCodeGuruProfilerAgentAccess 238
使用此政策 238
政策詳細資訊 238
政策版本 238
JSON 政策文件 238
進一步了解 239
AmazonCodeGuruProfilerFullAccess 239
使用此政策 239
政策詳細資訊 239
政策版本 240
JSON 政策文件 240
進一步了解 240
AmazonCodeGuruProfilerReadOnlyAccess 241
使用此政策 241
政策詳細資訊 241
政策版本 241
JSON 政策文件 241
進一步了解 242
AmazonCodeGuruReviewerFullAccess 242
使用此政策 242
政策詳細資訊 242
政策版本 242
JSON 政策文件 243
進一步了解 245

AmazonCodeGuruReviewerReadOnlyAccess 245
使用此政策 246
政策詳細資訊 246
政策版本 246
JSON 政策文件 246
進一步了解 246
AmazonCodeGuruReviewerServiceRolePolicy 247
使用此政策 247
政策詳細資訊 247
政策版本 247
JSON 政策文件 247
進一步了解 249
AmazonCodeGuruSecurityFullAccess 249
使用此政策 250
政策詳細資訊 250
政策版本 250
JSON 政策文件 250
進一步了解 250
AmazonCodeGuruSecurityScanAccess 251
使用此政策 251
政策詳細資訊 251
政策版本 251
JSON 政策文件 251
進一步了解 252
AmazonCognitoDeveloperAuthenticatedIdentities 252
使用此政策 252
政策詳細資訊 252
政策版本 252
JSON 政策文件 253
進一步了解 253
AmazonCognitoIdpEmailServiceRolePolicy 253
使用此政策 253
政策詳細資訊 253
政策版本 254
JSON 政策文件 254
進一步了解 254

AmazonCognitoIdpServiceRolePolicy 255
使用此政策 255
政策詳細資訊 255
政策版本 255
JSON 政策文件 255
進一步了解 256
AmazonCognitoPowerUser 256
使用此政策 256
政策詳細資訊 256
政策版本 256
JSON 政策文件 256
進一步了解 258
AmazonCognitoReadOnly 258
使用此政策 258
政策詳細資訊 258
政策版本 258
JSON 政策文件 259
進一步了解 259
AmazonCognitoUnAuthedIdentitiesSessionPolicy 260
使用此政策 260
政策詳細資訊 260
政策版本 260
JSON 政策文件 260
進一步了解 261
AmazonCognitoUnauthenticatedIdentities 261
使用此政策 262
政策詳細資訊 262
政策版本 262
JSON 政策文件 262
進一步了解 262
AmazonConnect_FullAccess 263
使用此政策 263
政策詳細資訊 263
政策版本 263
JSON 政策文件 263
進一步了解 266

AmazonConnectCampaignsServiceLinkedRolePolicy 266
使用此政策 266
政策詳細資訊 266
政策版本 267
JSON 政策文件 267
進一步了解 269
AmazonConnectReadOnlyAccess 269
使用此政策 269
政策詳細資訊 269
政策版本 269
JSON 政策文件 270
進一步了解 270
AmazonConnectServiceLinkedRolePolicy 270
使用此政策 271
政策詳細資訊 271
政策版本 271
JSON 政策文件 271
進一步了解 284
AmazonConnectSynchronizationServiceRolePolicy 284
使用此政策 284
政策詳細資訊 284
政策版本 284
JSON 政策文件 284
進一步了解 286
AmazonConnectVoiceIDFullAccess 286
使用此政策 287
政策詳細資訊 287
政策版本 287
JSON 政策文件 287
進一步了解 287
AmazonDataZoneBedrockModelConsumptionPolicy 288
使用此政策 288
政策詳細資訊 288
政策版本 288
JSON 政策文件 288
進一步了解 291

AmazonDataZoneBedrockModelManagementPolicy 291
使用此政策 291
政策詳細資訊 291
政策版本 291
JSON 政策文件 291
進一步了解 293
AmazonDataZoneDomainExecutionRolePolicy 293
使用此政策 294
政策詳細資訊 294
政策版本 294
JSON 政策文件 294
進一步了解 298
AmazonDataZoneEnvironmentRolePermissionsBoundary 298
使用此政策 298
政策詳細資訊 298
政策版本 298
JSON 政策文件 299
進一步了解 311
AmazonDataZoneFullAccess 312
使用此政策 312
政策詳細資訊 312
政策版本 312
JSON 政策文件 312
進一步了解 321
AmazonDataZoneFullUserAccess 321
使用此政策 321
政策詳細資訊 322
政策版本 322
JSON 政策文件 322
進一步了解 325
AmazonDataZoneGlueManageAccessRolePolicy 326
使用此政策 326
政策詳細資訊 326
政策版本 326
JSON 政策文件 326
進一步了解 334

AmazonDataZonePortalFullAccessPolicy 334
使用此政策 334
政策詳細資訊 334
政策版本 335
JSON 政策文件 335
進一步了解 335
AmazonDataZonePreviewConsoleFullAccess 335
使用此政策 335
政策詳細資訊 336
政策版本 336
JSON 政策文件 336
進一步了解 338
AmazonDataZoneProjectDeploymentPermissionsBoundary 338
使用此政策 338
政策詳細資訊 338
政策版本 338
JSON 政策文件 339
進一步了解 347
AmazonDataZoneProjectRolePermissionsBoundary 347
使用此政策 347
政策詳細資訊 347
政策版本 347
JSON 政策文件 347
進一步了解 355
AmazonDataZoneRedshiftGlueProvisioningPolicy 355
使用此政策 355
政策詳細資訊 355
政策版本 355
JSON 政策文件 355
進一步了解 363
AmazonDataZoneRedshiftManageAccessRolePolicy 363
使用此政策 364
政策詳細資訊 364
政策版本 364
JSON 政策文件 364
進一步了解 367

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 367
使用此政策 368
政策詳細資訊 368
政策版本 368
JSON 政策文件 368
進一步了解 395
AmazonDataZoneSageMakerManageAccessRolePolicy 396
使用此政策 396
政策詳細資訊 396
政策版本 396
JSON 政策文件 396
進一步了解 401
AmazonDataZoneSageMakerProvisioningRolePolicy 401
使用此政策 401
政策詳細資訊 401
政策版本 402
JSON 政策文件 402
進一步了解 406
AmazonDetectiveFullAccess 407
使用此政策 407
政策詳細資訊 407
政策版本 407
JSON 政策文件 407
進一步了解 408
AmazonDetectiveInvestigatorAccess 408
使用此政策 409
政策詳細資訊 409
政策版本 409
JSON 政策文件 409
進一步了解 411
AmazonDetectiveMemberAccess 411
使用此政策 411
政策詳細資訊 411
政策版本 411
JSON 政策文件 411
進一步了解 412

AmazonDetectiveOrganizationsAccess 412
使用此政策 412
政策詳細資訊 412
政策版本 413
JSON 政策文件 413
進一步了解 414
AmazonDetectiveServiceLinkedRolePolicy 415
使用此政策 415
政策詳細資訊 415
政策版本 415
JSON 政策文件 415
進一步了解 416
AmazonDevOpsGuruConsoleFullAccess 416
使用此政策 416
政策詳細資訊 416
政策版本 416
JSON 政策文件 417
進一步了解 419
AmazonDevOpsGuruFullAccess 419
使用此政策 419
政策詳細資訊 419
政策版本 420
JSON 政策文件 420
進一步了解 422
AmazonDevOpsGuruOrganizationsAccess 422
使用此政策 422
政策詳細資訊 422
政策版本 423
JSON 政策文件 423
進一步了解 424
AmazonDevOpsGuruReadOnlyAccess 424
使用此政策 424
政策詳細資訊 425
政策版本 425
JSON 政策文件 425
進一步了解 427

AmazonDevOpsGuruServiceRolePolicy 427
使用此政策 427
政策詳細資訊 427
政策版本 427
JSON 政策文件 428
進一步了解 432
AmazonDMSCloudWatchLogsRole 432
使用此政策 432
政策詳細資訊 432
政策版本 432
JSON 政策文件 432
進一步了解 434
AmazonDMSRedshiftS3Role 434
使用此政策 434
政策詳細資訊 434
政策版本 435
JSON 政策文件 435
進一步了解 435
AmazonDMSVPCManagementRole 436
使用此政策 436
政策詳細資訊 436
政策版本 436
JSON 政策文件 436
進一步了解 437
AmazonDocDB-ElasticServiceRolePolicy 437
使用此政策 437
政策詳細資訊 437
政策版本 438
JSON 政策文件 438
進一步了解 438
AmazonDocDBConsoleFullAccess 438
使用此政策 439
政策詳細資訊 439
政策版本 439
JSON 政策文件 439
進一步了解 443

AmazonDocDBElasticFullAccess 444
使用此政策 444
政策詳細資訊 444
政策版本 444
JSON 政策文件 444
進一步了解 448
AmazonDocDBElasticReadOnlyAccess 448
使用此政策 448
政策詳細資訊 448
政策版本 448
JSON 政策文件 448
進一步了解 449
AmazonDocDBFullAccess 449
使用此政策 449
政策詳細資訊 450
政策版本 450
JSON 政策文件 450
進一步了解 453
AmazonDocDBReadOnlyAccess 453
使用此政策 453
政策詳細資訊 453
政策版本 453
JSON 政策文件 453
進一步了解 455
AmazonDRSVPCManagement 455
使用此政策 456
政策詳細資訊 456
政策版本 456
JSON 政策文件 456
進一步了解 457
AmazonDynamoDBFullAccess 457
使用此政策 457
政策詳細資訊 457
政策版本 457
JSON 政策文件 458
進一步了解 460

AmazonDynamoDBFullAccess_v2 460
使用此政策 460
政策詳細資訊 461
政策版本 461
JSON 政策文件 461
進一步了解 464
AmazonDynamoDBFullAccesswithDataPipeline 464
使用此政策 465
政策詳細資訊 465
政策版本 465
JSON 政策文件 465
進一步了解 467
AmazonDynamoDBReadOnlyAccess 467
使用此政策 467
政策詳細資訊 468
政策版本 468
JSON 政策文件 468
進一步了解 470
AmazonEBSCSIDriverPolicy 470
使用此政策 470
政策詳細資訊 470
政策版本 470
JSON 政策文件 470
進一步了解 475
AmazonEC2ContainerRegistryFullAccess 475
使用此政策 475
政策詳細資訊 475
政策版本 476
JSON 政策文件 476
進一步了解 476
AmazonEC2ContainerRegistryPowerUser 477
使用此政策 477
政策詳細資訊 477
政策版本 477
JSON 政策文件 477
進一步了解 478

AmazonEC2ContainerRegistryPullOnly 478
使用此政策 478
政策詳細資訊 478
政策版本 479
JSON 政策文件 479
進一步了解 479
AmazonEC2ContainerRegistryReadOnly 479
使用此政策 480
政策詳細資訊 480
政策版本 480
JSON 政策文件 480
進一步了解 481
AmazonEC2ContainerServiceAutoscaleRole 481
使用此政策 481
政策詳細資訊 481
政策版本 481
JSON 政策文件 482
進一步了解 482
AmazonEC2ContainerServiceEventsRole 482
使用此政策 483
政策詳細資訊 483
政策版本 483
JSON 政策文件 483
進一步了解 484
AmazonEC2ContainerServiceforEC2Role 484
使用此政策 484
政策詳細資訊 484
政策版本 485
JSON 政策文件 485
進一步了解 486
AmazonEC2ContainerServiceRole 486
使用此政策 486
政策詳細資訊 487
政策版本 487
JSON 政策文件 487
進一步了解 487

AmazonEC2FullAccess 488
使用此政策 488
政策詳細資訊 488
政策版本 488
JSON 政策文件 488
進一步了解 489
AmazonEC2ImageReferencesAccessPolicy 490
使用此政策 490
政策詳細資訊 490
政策版本 490
JSON 政策文件 490
進一步了解 491
AmazonEC2ReadOnlyAccess 491
使用此政策 491
政策詳細資訊 491
政策版本 492
JSON 政策文件 492
進一步了解 493
AmazonEC2RoleforAWSCodeDeploy 493
使用此政策 493
政策詳細資訊 493
政策版本 493
JSON 政策文件 494
進一步了解 494
AmazonEC2RoleforAWSCodeDeployLimited 494
使用此政策 494
政策詳細資訊 494
政策版本 495
JSON 政策文件 495
進一步了解 496
AmazonEC2RoleforDataPipelineRole 496
使用此政策 496
政策詳細資訊 496
政策版本 496
JSON 政策文件 496
進一步了解 497

AmazonEC2RoleforSSM 497
使用此政策 498
政策詳細資訊 498
政策版本 498
JSON 政策文件 498
進一步了解 500
AmazonEC2RolePolicyForLaunchWizard 500
使用此政策 501
政策詳細資訊 501
政策版本 501
JSON 政策文件 501
進一步了解 505
AmazonEC2SpotFleetAutoscaleRole 505
使用此政策 505
政策詳細資訊 505
政策版本 506
JSON 政策文件 506
進一步了解 507
AmazonEC2SpotFleetTaggingRole 507
使用此政策 507
政策詳細資訊 507
政策版本 507
JSON 政策文件 508
進一步了解 509
AmazonECS_FullAccess 509
使用此政策 509
政策詳細資訊 509
政策版本 510
JSON 政策文件 510
進一步了解 515
AmazonECSComputeServiceRolePolicy 516
使用此政策 516
政策詳細資訊 516
政策版本 516
JSON 政策文件 516
進一步了解 518

AmazonECSInfrastructureRoleforExpressGatewayServices 518
使用此政策 518
政策詳細資訊 518
政策版本 519
JSON 政策文件 519
進一步了解 525
AmazonECSInfrastructureRolePolicyForLoadBalancers 525
使用此政策 525
政策詳細資訊 526
政策版本 526
JSON 政策文件 526
進一步了解 527
AmazonECSInfrastructureRolePolicyForManagedInstances 527
使用此政策 528
政策詳細資訊 528
政策版本 528
JSON 政策文件 528
進一步了解 532
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 533
使用此政策 533
政策詳細資訊 533
政策版本 533
JSON 政策文件 533
進一步了解 536
AmazonECSInfrastructureRolePolicyForVolumes 536
使用此政策 536
政策詳細資訊 536
政策版本 537
JSON 政策文件 537
進一步了解 539
AmazonECSInfrastructureRolePolicyForVpcLattice 539
使用此政策 539
政策詳細資訊 539
政策版本 540
JSON 政策文件 540
進一步了解 541

AmazonECSInstanceRolePolicyForManagedInstances 541
使用此政策 541
政策詳細資訊 541
政策版本 542
JSON 政策文件 542
進一步了解 543
AmazonECSServiceRolePolicy 543
使用此政策 543
政策詳細資訊 543
政策版本 544
JSON 政策文件 544
進一步了解 549
AmazonECSTaskExecutionRolePolicy 550
使用此政策 550
政策詳細資訊 550
政策版本 550
JSON 政策文件 550
進一步了解 551
AmazonEFSCSIDriverPolicy 551
使用此政策 551
政策詳細資訊 551
政策版本 551
JSON 政策文件 552
進一步了解 553
AmazonEKS_CNI_Policy 553
使用此政策 553
政策詳細資訊 554
政策版本 554
JSON 政策文件 554
進一步了解 555
AmazonEKSBlockStoragePolicy 555
使用此政策 555
政策詳細資訊 555
政策版本 555
JSON 政策文件 556
進一步了解 558

AmazonEKSClusterPolicy 558
使用此政策 558
政策詳細資訊 558
政策版本 559
JSON 政策文件 559
進一步了解 561
AmazonEKSComputePolicy 561
使用此政策 561
政策詳細資訊 561
政策版本 562
JSON 政策文件 562
進一步了解 564
AmazonEKSConnectorServiceRolePolicy 565
使用此政策 565
政策詳細資訊 565
政策版本 565
JSON 政策文件 565
進一步了解 567
AmazonEKSDashboardConsoleReadOnly 567
使用此政策 568
政策詳細資訊 568
政策版本 568
JSON 政策文件 568
進一步了解 569
AmazonEKSDashboardServiceRolePolicy 569
使用此政策 570
政策詳細資訊 570
政策版本 570
JSON 政策文件 570
進一步了解 571
AmazonEKSFargatePodExecutionRolePolicy 571
使用此政策 571
政策詳細資訊 571
政策版本 571
JSON 政策文件 571
進一步了解 572

AmazonEKSForFargateServiceRolePolicy 572
使用此政策 572
政策詳細資訊 572
政策版本 573
JSON 政策文件 573
進一步了解 573
AmazonEKSLoadBalancingPolicy 573
使用此政策 574
政策詳細資訊 574
政策版本 574
JSON 政策文件 574
進一步了解 580
AmazonEKSLocalOutpostClusterPolicy 580
使用此政策 580
政策詳細資訊 581
政策版本 581
JSON 政策文件 581
進一步了解 583
AmazonEKSLocalOutpostServiceRolePolicy 583
使用此政策 583
政策詳細資訊 583
政策版本 583
JSON 政策文件 584
進一步了解 589
AmazonEKSMCPReadOnlyAccess 589
使用此政策 590
政策詳細資訊 590
政策版本 590
JSON 政策文件 590
進一步了解 592
AmazonEKSNetworkingPolicy 592
使用此政策 592
政策詳細資訊 592
政策版本 592
JSON 政策文件 593
進一步了解 594

AmazonEKSServicePolicy 595
使用此政策 595
政策詳細資訊 595
政策版本 595
JSON 政策文件 595
進一步了解 597
AmazonEKSServiceRolePolicy 597
使用此政策 598
政策詳細資訊 598
政策版本 598
JSON 政策文件 598
進一步了解 606
AmazonEKSVPCResourceController 606
使用此政策 606
政策詳細資訊 606
政策版本 606
JSON 政策文件 607
進一步了解 607
AmazonEKSWorkerNodeMinimalPolicy 608
使用此政策 608
政策詳細資訊 608
政策版本 608
JSON 政策文件 608
進一步了解 609
AmazonEKSWorkerNodePolicy 609
使用此政策 609
政策詳細資訊 609
政策版本 609
JSON 政策文件 609
進一步了解 610
AmazonElastiCacheFullAccess 610
使用此政策 610
政策詳細資訊 610
政策版本 611
JSON 政策文件 611
進一步了解 614

AmazonElastiCacheReadOnlyAccess 614
使用此政策 614
政策詳細資訊 614
政策版本 615
JSON 政策文件 615
進一步了解 615
AmazonElasticContainerRegistryPublicFullAccess 615
使用此政策 616
政策詳細資訊 616
政策版本 616
JSON 政策文件 616
進一步了解 616
AmazonElasticContainerRegistryPublicPowerUser 617
使用此政策 617
政策詳細資訊 617
政策版本 617
JSON 政策文件 617
進一步了解 618
AmazonElasticContainerRegistryPublicReadOnly 618
使用此政策 618
政策詳細資訊 618
政策版本 619
JSON 政策文件 619
進一步了解 619
AmazonElasticFileSystemClientFullAccess 620
使用此政策 620
政策詳細資訊 620
政策版本 620
JSON 政策文件 620
進一步了解 621
AmazonElasticFileSystemClientReadOnlyAccess 621
使用此政策 621
政策詳細資訊 621
政策版本 621
JSON 政策文件 621
進一步了解 622

AmazonElasticFileSystemClientReadWriteAccess 622
使用此政策 622
政策詳細資訊 622
政策版本 622
JSON 政策文件 623
進一步了解 623
AmazonElasticFileSystemFullAccess 623
使用此政策 623
政策詳細資訊 623
政策版本 624
JSON 政策文件 624
進一步了解 626
AmazonElasticFileSystemReadOnlyAccess 626
使用此政策 626
政策詳細資訊 626
政策版本 627
JSON 政策文件 627
進一步了解 628
AmazonElasticFileSystemServiceRolePolicy 628
使用此政策 628
政策詳細資訊 628
政策版本 628
JSON 政策文件 628
進一步了解 631
AmazonElasticFileSystemsUtils 631
使用此政策 631
政策詳細資訊 631
政策版本 631
JSON 政策文件 631
進一步了解 633
AmazonElasticMapReduceEditorsRole 633
使用此政策 633
政策詳細資訊 634
政策版本 634
JSON 政策文件 634
進一步了解 635

AmazonElasticMapReduceforAutoScalingRole 635
使用此政策 635
政策詳細資訊 636
政策版本 636
JSON 政策文件 636
進一步了解 636
AmazonElasticMapReduceforEC2Role 637
使用此政策 637
政策詳細資訊 637
政策版本 637
JSON 政策文件 637
進一步了解 639
AmazonElasticMapReduceFullAccess 639
使用此政策 639
政策詳細資訊 639
政策版本 639
JSON 政策文件 640
進一步了解 641
AmazonElasticMapReducePlacementGroupPolicy 641
使用此政策 641
政策詳細資訊 642
政策版本 642
JSON 政策文件 642
進一步了解 642
AmazonElasticMapReduceReadOnlyAccess 643
使用此政策 643
政策詳細資訊 643
政策版本 643
JSON 政策文件 643
進一步了解 644
AmazonElasticMapReduceRole 644
使用此政策 644
政策詳細資訊 644
政策版本 645
JSON 政策文件 645
進一步了解 647

AmazonElasticsearchServiceRolePolicy 647
使用此政策 647
政策詳細資訊 647
政策版本 648
JSON 政策文件 648
進一步了解 650
AmazonElasticTranscoder_FullAccess 651
使用此政策 651
政策詳細資訊 651
政策版本 651
JSON 政策文件 651
進一步了解 652
AmazonElasticTranscoder_JobsSubmitter 652
使用此政策 652
政策詳細資訊 652
政策版本 653
JSON 政策文件 653
進一步了解 653
AmazonElasticTranscoder_ReadOnlyAccess 654
使用此政策 654
政策詳細資訊 654
政策版本 654
JSON 政策文件 654
進一步了解 655
AmazonElasticTranscoderRole 655
使用此政策 655
政策詳細資訊 655
政策版本 655
JSON 政策文件 655
進一步了解 656
AmazonEMRCleanupPolicy 656
使用此政策 657
政策詳細資訊 657
政策版本 657
JSON 政策文件 657
進一步了解 658

AmazonEMRContainersServiceRolePolicy 658
使用此政策 658
政策詳細資訊 658
政策版本 658
JSON 政策文件 659
進一步了解 660
AmazonEMRFullAccessPolicy_v2 660
使用此政策 660
政策詳細資訊 660
政策版本 660
JSON 政策文件 661
進一步了解 664
AmazonEMRReadOnlyAccessPolicy_v2 664
使用此政策 664
政策詳細資訊 664
政策版本 665
JSON 政策文件 665
進一步了解 666
AmazonEMRServerlessServiceRolePolicy 666
使用此政策 666
政策詳細資訊 666
政策版本 666
JSON 政策文件 667
進一步了解 668
AmazonEMRServicePolicy_v2 668
使用此政策 668
政策詳細資訊 668
政策版本 668
JSON 政策文件 668
進一步了解 677
AmazonESCognitoAccess 677
使用此政策 677
政策詳細資訊 677
政策版本 678
JSON 政策文件 678
進一步了解 679

AmazonESFullAccess 679
使用此政策 679
政策詳細資訊 679
政策版本 679
JSON 政策文件 680
進一步了解 680
AmazonESReadOnlyAccess 680
使用此政策 680
政策詳細資訊 680
政策版本 681
JSON 政策文件 681
進一步了解 681
AmazonEventBridgeApiDestinationsServiceRolePolicy 681
使用此政策 682
政策詳細資訊 682
政策版本 682
JSON 政策文件 682
進一步了解 683
AmazonEventBridgeFullAccess 683
使用此政策 683
政策詳細資訊 684
政策版本 684
JSON 政策文件 684
進一步了解 686
AmazonEventBridgePipesFullAccess 686
使用此政策 686
政策詳細資訊 686
政策版本 687
JSON 政策文件 687
進一步了解 687
AmazonEventBridgePipesOperatorAccess 688
使用此政策 688
政策詳細資訊 688
政策版本 688
JSON 政策文件 688
進一步了解 689

AmazonEventBridgePipesReadOnlyAccess 689
使用此政策 689
政策詳細資訊 689
政策版本 689
JSON 政策文件 690
進一步了解 690
AmazonEventBridgeReadOnlyAccess 690
使用此政策 690
政策詳細資訊 690
政策版本 691
JSON 政策文件 691
進一步了解 692
AmazonEventBridgeSchedulerFullAccess 692
使用此政策 692
政策詳細資訊 693
政策版本 693
JSON 政策文件 693
進一步了解 693
AmazonEventBridgeSchedulerReadOnlyAccess 694
使用此政策 694
政策詳細資訊 694
政策版本 694
JSON 政策文件 694
進一步了解 695
AmazonEventBridgeSchemasFullAccess 695
使用此政策 695
政策詳細資訊 695
政策版本 695
JSON 政策文件 696
進一步了解 697
AmazonEventBridgeSchemasReadOnlyAccess 697
使用此政策 697
政策詳細資訊 697
政策版本 697
JSON 政策文件 697
進一步了解 698

AmazonEventBridgeSchemasServiceRolePolicy 698
使用此政策 698
政策詳細資訊 699
政策版本 699
JSON 政策文件 699
進一步了解 700
AmazonEVSServiceRolePolicy 700
使用此政策 700
政策詳細資訊 700
政策版本 700
JSON 政策文件 700
進一步了解 704
AmazonFISServiceRolePolicy 704
使用此政策 704
政策詳細資訊 705
政策版本 705
JSON 政策文件 705
進一步了解 707
AmazonForecastFullAccess 707
使用此政策 707
政策詳細資訊 707
政策版本 707
JSON 政策文件 707
進一步了解 708
AmazonFraudDetectorFullAccessPolicy 708
使用此政策 708
政策詳細資訊 708
政策版本 709
JSON 政策文件 709
進一步了解 710
AmazonFreeRTOSFullAccess 710
使用此政策 710
政策詳細資訊 710
政策版本 711
JSON 政策文件 711
進一步了解 711

AmazonFreeRTOSOTAUpdate 711
使用此政策 712
政策詳細資訊 712
政策版本 712
JSON 政策文件 712
進一步了解 713
AmazonFSxConsoleFullAccess 714
使用此政策 714
政策詳細資訊 714
政策版本 714
JSON 政策文件 714
進一步了解 718
AmazonFSxConsoleReadOnlyAccess 718
使用此政策 718
政策詳細資訊 718
政策版本 718
JSON 政策文件 719
進一步了解 719
AmazonFSxFullAccess 719
使用此政策 720
政策詳細資訊 720
政策版本 720
JSON 政策文件 720
進一步了解 724
AmazonFSxReadOnlyAccess 724
使用此政策 724
政策詳細資訊 725
政策版本 725
JSON 政策文件 725
進一步了解 725
AmazonFSxServiceRolePolicy 726
使用此政策 726
政策詳細資訊 726
政策版本 726
JSON 政策文件 726
進一步了解 729

AmazonGlacierFullAccess 729
使用此政策 729
政策詳細資訊 729
政策版本 730
JSON 政策文件 730
進一步了解 730
AmazonGlacierReadOnlyAccess 730
使用此政策 730
政策詳細資訊 730
政策版本 731
JSON 政策文件 731
進一步了解 731
AmazonGrafanaAthenaAccess 732
使用此政策 732
政策詳細資訊 732
政策版本 732
JSON 政策文件 732
進一步了解 734
AmazonGrafanaCloudWatchAccess 734
使用此政策 734
政策詳細資訊 735
政策版本 735
JSON 政策文件 735
進一步了解 736
AmazonGrafanaRedshiftAccess 736
使用此政策 737
政策詳細資訊 737
政策版本 737
JSON 政策文件 737
進一步了解 738
AmazonGrafanaServiceLinkedRolePolicy 739
使用此政策 739
政策詳細資訊 739
政策版本 739
JSON 政策文件 739
進一步了解 740

AmazonGuardDutyFullAccess 741
使用此政策 741
政策詳細資訊 741
政策版本 741
JSON 政策文件 741
進一步了解 743
AmazonGuardDutyFullAccess_v2 743
使用此政策 743
政策詳細資訊 743
政策版本 743
JSON 政策文件 744
進一步了解 745
AmazonGuardDutyMalwareProtectionServiceRolePolicy 746
使用此政策 746
政策詳細資訊 746
政策版本 746
JSON 政策文件 746
進一步了解 751
AmazonGuardDutyReadOnlyAccess 751
使用此政策 751
政策詳細資訊 751
政策版本 751
JSON 政策文件 752
進一步了解 752
AmazonGuardDutyServiceRolePolicy 753
使用此政策 753
政策詳細資訊 753
政策版本 753
JSON 政策文件 753
進一步了解 759
AmazonHealthLakeFullAccess 759
使用此政策 760
政策詳細資訊 760
政策版本 760
JSON 政策文件 760
進一步了解 761

AmazonHealthLakeReadOnlyAccess 761
使用此政策 761
政策詳細資訊 761
政策版本 761
JSON 政策文件 762
進一步了解 762
AmazonHoneycodeFullAccess 762
使用此政策 762
政策詳細資訊 763
政策版本 763
JSON 政策文件 763
進一步了解 763
AmazonHoneycodeReadOnlyAccess 764
使用此政策 764
政策詳細資訊 764
政策版本 764
JSON 政策文件 764
進一步了解 765
AmazonHoneycodeServiceRolePolicy 765
使用此政策 765
政策詳細資訊 765
政策版本 765
JSON 政策文件 765
進一步了解 766
AmazonHoneycodeTeamAssociationFullAccess 766
使用此政策 766
政策詳細資訊 766
政策版本 766
JSON 政策文件 767
進一步了解 767
AmazonHoneycodeTeamAssociationReadOnlyAccess 767
使用此政策 767
政策詳細資訊 767
政策版本 768
JSON 政策文件 768
進一步了解 768

AmazonHoneycodeWorkbookFullAccess 768
使用此政策 769
政策詳細資訊 769
政策版本 769
JSON 政策文件 769
進一步了解 770
AmazonHoneycodeWorkbookReadOnlyAccess 770
使用此政策 770
政策詳細資訊 770
政策版本 770
JSON 政策文件 770
進一步了解 771
AmazonInspector2AgentlessServiceRolePolicy 771
使用此政策 771
政策詳細資訊 771
政策版本 772
JSON 政策文件 772
進一步了解 775
AmazonInspector2FullAccess 776
使用此政策 776
政策詳細資訊 776
政策版本 776
JSON 政策文件 776
進一步了解 777
AmazonInspector2FullAccess_v2 778
使用此政策 778
政策詳細資訊 778
政策版本 778
JSON 政策文件 778
進一步了解 781
AmazonInspector2ManagedCisPolicy 781
使用此政策 781
政策詳細資訊 781
政策版本 781
JSON 政策文件 782
進一步了解 782

AmazonInspector2ManagedTelemetryPolicy 782
使用此政策 782
政策詳細資訊 783
政策版本 783
JSON 政策文件 783
進一步了解 783
AmazonInspector2ReadOnlyAccess 784
使用此政策 784
政策詳細資訊 784
政策版本 784
JSON 政策文件 784
進一步了解 786
AmazonInspector2ServiceRolePolicy 786
使用此政策 786
政策詳細資訊 786
政策版本 786
JSON 政策文件 786
進一步了解 794
AmazonInspectorFullAccess 795
使用此政策 795
政策詳細資訊 795
政策版本 795
JSON 政策文件 795
進一步了解 796
AmazonInspectorReadOnlyAccess 796
使用此政策 797
政策詳細資訊 797
政策版本 797
JSON 政策文件 797
進一步了解 798
AmazonInspectorServiceRolePolicy 798
使用此政策 798
政策詳細資訊 798
政策版本 798
JSON 政策文件 799
進一步了解 800

AmazonKendraFullAccess 800
使用此政策 800
政策詳細資訊 800
政策版本 800
JSON 政策文件 801
進一步了解 802
AmazonKendraReadOnlyAccess 803
使用此政策 803
政策詳細資訊 803
政策版本 803
JSON 政策文件 803
進一步了解 804
AmazonKeyspacesFullAccess 804
使用此政策 804
政策詳細資訊 804
政策版本 804
JSON 政策文件 805
進一步了解 807
AmazonKeyspacesReadOnlyAccess 807
使用此政策 807
政策詳細資訊 807
政策版本 807
JSON 政策文件 807
進一步了解 808
AmazonKeyspacesReadOnlyAccess_v2 808
使用此政策 809
政策詳細資訊 809
政策版本 809
JSON 政策文件 809
進一步了解 810
AmazonKinesisAnalyticsFullAccess 810
使用此政策 810
政策詳細資訊 810
政策版本 811
JSON 政策文件 811
進一步了解 812

AmazonKinesisAnalyticsReadOnly 812
使用此政策 813
政策詳細資訊 813
政策版本 813
JSON 政策文件 813
進一步了解 814
AmazonKinesisFirehoseFullAccess 815
使用此政策 815
政策詳細資訊 815
政策版本 815
JSON 政策文件 815
進一步了解 816
AmazonKinesisFirehoseReadOnlyAccess 816
使用此政策 816
政策詳細資訊 816
政策版本 816
JSON 政策文件 816
進一步了解 817
AmazonKinesisFullAccess 817
使用此政策 817
政策詳細資訊 817
政策版本 817
JSON 政策文件 818
進一步了解 818
AmazonKinesisReadOnlyAccess 818
使用此政策 818
政策詳細資訊 818
政策版本 819
JSON 政策文件 819
進一步了解 819
AmazonKinesisVideoStreamsFullAccess 819
使用此政策 820
政策詳細資訊 820
政策版本 820
JSON 政策文件 820
進一步了解 820

AmazonKinesisVideoStreamsReadOnlyAccess 821
使用此政策 821
政策詳細資訊 821
政策版本 821
JSON 政策文件 821
進一步了解 822
AmazonLaunchWizard_Fullaccess 822
使用此政策 822
政策詳細資訊 822
政策版本 822
JSON 政策文件 823
進一步了解 837
AmazonLaunchWizardFullAccessV2 837
使用此政策 837
政策詳細資訊 837
政策版本 837
JSON 政策文件 838
進一步了解 854
AmazonLexChannelsAccess 854
使用此政策 854
政策詳細資訊 855
政策版本 855
JSON 政策文件 855
進一步了解 855
AmazonLexFullAccess 855
使用此政策 856
政策詳細資訊 856
政策版本 856
JSON 政策文件 856
進一步了解 862
AmazonLexReadOnly 862
使用此政策 862
政策詳細資訊 862
政策版本 862
JSON 政策文件 862
進一步了解 864

AmazonLexReplicationPolicy 864
使用此政策 864
政策詳細資訊 864
政策版本 865
JSON 政策文件 865
進一步了解 867
AmazonLexRunBotsOnly 867
使用此政策 867
政策詳細資訊 867
政策版本 868
JSON 政策文件 868
進一步了解 868
AmazonLexV2BotPolicy 868
使用此政策 869
政策詳細資訊 869
政策版本 869
JSON 政策文件 869
進一步了解 870
AmazonLookoutEquipmentFullAccess 870
使用此政策 870
政策詳細資訊 870
政策版本 870
JSON 政策文件 870
進一步了解 871
AmazonLookoutEquipmentReadOnlyAccess 872
使用此政策 872
政策詳細資訊 872
政策版本 872
JSON 政策文件 872
進一步了解 873
AmazonLookoutMetricsFullAccess 873
使用此政策 873
政策詳細資訊 873
政策版本 873
JSON 政策文件 874
進一步了解 874

AmazonLookoutMetricsReadOnlyAccess 874
使用此政策 875
政策詳細資訊 875
政策版本 875
JSON 政策文件 875
進一步了解 876
AmazonLookoutVisionConsoleFullAccess 876
使用此政策 876
政策詳細資訊 876
政策版本 876
JSON 政策文件 877
進一步了解 879
AmazonLookoutVisionConsoleReadOnlyAccess 879
使用此政策 879
政策詳細資訊 879
政策版本 879
JSON 政策文件 880
進一步了解 881
AmazonLookoutVisionFullAccess 881
使用此政策 881
政策詳細資訊 881
政策版本 882
JSON 政策文件 882
進一步了解 882
AmazonLookoutVisionReadOnlyAccess 882
使用此政策 882
政策詳細資訊 883
政策版本 883
JSON 政策文件 883
進一步了解 884
AmazonMachineLearningBatchPredictionsAccess 884
使用此政策 884
政策詳細資訊 884
政策版本 884
JSON 政策文件 884
進一步了解 885

AmazonMachineLearningCreateOnlyAccess 885
使用此政策 885
政策詳細資訊 885
政策版本 886
JSON 政策文件 886
進一步了解 886
AmazonMachineLearningFullAccess 886
使用此政策 887
政策詳細資訊 887
政策版本 887
JSON 政策文件 887
進一步了解 887
AmazonMachineLearningManageRealTimeEndpointOnlyAccess 888
使用此政策 888
政策詳細資訊 888
政策版本 888
JSON 政策文件 888
進一步了解 889
AmazonMachineLearningReadOnlyAccess 889
使用此政策 889
政策詳細資訊 889
政策版本 889
JSON 政策文件 890
進一步了解 890
AmazonMachineLearningRealTimePredictionOnlyAccess 890
使用此政策 890
政策詳細資訊 890
政策版本 891
JSON 政策文件 891
進一步了解 891
AmazonMachineLearningRoleforRedshiftDataSourceV3 891
使用此政策 892
政策詳細資訊 892
政策版本 892
JSON 政策文件 892
進一步了解 893

AmazonMacieFullAccess 893
使用此政策 893
政策詳細資訊 893
政策版本 894
JSON 政策文件 894
進一步了解 894
AmazonMacieHandshakeRole 895
使用此政策 895
政策詳細資訊 895
政策版本 895
JSON 政策文件 895
進一步了解 896
AmazonMacieReadOnlyAccess 896
使用此政策 896
政策詳細資訊 896
政策版本 896
JSON 政策文件 897
進一步了解 897
AmazonMacieServiceRole 897
使用此政策 897
政策詳細資訊 897
政策版本 898
JSON 政策文件 898
進一步了解 898
AmazonMacieServiceRolePolicy 898
使用此政策 899
政策詳細資訊 899
政策版本 899
JSON 政策文件 899
進一步了解 900
AmazonManagedBlockchainConsoleFullAccess 901
使用此政策 901
政策詳細資訊 901
政策版本 901
JSON 政策文件 901
進一步了解 902

AmazonManagedBlockchainFullAccess 902
使用此政策 902
政策詳細資訊 902
政策版本 902
JSON 政策文件 903
進一步了解 903
AmazonManagedBlockchainReadOnlyAccess 903
使用此政策 903
政策詳細資訊 903
政策版本 904
JSON 政策文件 904
進一步了解 904
AmazonManagedBlockchainServiceRolePolicy 904
使用此政策 905
政策詳細資訊 905
政策版本 905
JSON 政策文件 905
進一步了解 906
AmazonMCSFullAccess 906
使用此政策 906
政策詳細資訊 906
政策版本 906
JSON 政策文件 907
進一步了解 908
AmazonMCSReadOnlyAccess 908
使用此政策 908
政策詳細資訊 908
政策版本 908
JSON 政策文件 909
進一步了解 909
AmazonMechanicalTurkFullAccess 909
使用此政策 910
政策詳細資訊 910
政策版本 910
JSON 政策文件 910
進一步了解 910

AmazonMechanicalTurkReadOnly 911
使用此政策 911
政策詳細資訊 911
政策版本 911
JSON 政策文件 911
進一步了解 912
AmazonMemoryDBFullAccess 912
使用此政策 912
政策詳細資訊 912
政策版本 912
JSON 政策文件 913
進一步了解 913
AmazonMemoryDBReadOnlyAccess 913
使用此政策 914
政策詳細資訊 914
政策版本 914
JSON 政策文件 914
進一步了解 914
AmazonMobileAnalyticsFinancialReportAccess 915
使用此政策 915
政策詳細資訊 915
政策版本 915
JSON 政策文件 915
進一步了解 916
AmazonMobileAnalyticsFullAccess 916
使用此政策 916
政策詳細資訊 916
政策版本 916
JSON 政策文件 916
進一步了解 917
AmazonMobileAnalyticsNon-financialReportAccess 917
使用此政策 917
政策詳細資訊 917
政策版本 917
JSON 政策文件 918
進一步了解 918

AmazonMobileAnalyticsWriteOnlyAccess 918
使用此政策 918
政策詳細資訊 918
政策版本 919
JSON 政策文件 919
進一步了解 919
AmazonMonitronFullAccess 919
使用此政策 919
政策詳細資訊 920
政策版本 920
JSON 政策文件 920
進一步了解 922
AmazonMQApiFullAccess 922
使用此政策 922
政策詳細資訊 922
政策版本 922
JSON 政策文件 923
進一步了解 924
AmazonMQApiReadOnlyAccess 924
使用此政策 924
政策詳細資訊 924
政策版本 924
JSON 政策文件 924
進一步了解 925
AmazonMQFullAccess 925
使用此政策 925
政策詳細資訊 925
政策版本 926
JSON 政策文件 926
進一步了解 927
AmazonMQReadOnlyAccess 927
使用此政策 927
政策詳細資訊 927
政策版本 928
JSON 政策文件 928
進一步了解 928

AmazonMQServiceRolePolicy 928
使用此政策 929
政策詳細資訊 929
政策版本 929
JSON 政策文件 929
進一步了解 931
AmazonMSKConnectReadOnlyAccess 931
使用此政策 931
政策詳細資訊 931
政策版本 931
JSON 政策文件 932
進一步了解 933
AmazonMSKFullAccess 933
使用此政策 933
政策詳細資訊 933
政策版本 933
JSON 政策文件 933
進一步了解 936
AmazonMSKReadOnlyAccess 936
使用此政策 936
政策詳細資訊 937
政策版本 937
JSON 政策文件 937
進一步了解 937
AmazonMWAAServerlessServiceRolePolicy 938
使用此政策 938
政策詳細資訊 938
政策版本 938
JSON 政策文件 938
進一步了解 939
AmazonMWAAServiceRolePolicy 939
使用此政策 939
政策詳細資訊 939
政策版本 940
JSON 政策文件 940
進一步了解 942

AmazonNimbleStudio-LaunchProfileWorker 942
使用此政策 942
政策詳細資訊 942
政策版本 943
JSON 政策文件 943
進一步了解 943
AmazonNimbleStudio-StudioAdmin 944
使用此政策 944
政策詳細資訊 944
政策版本 944
JSON 政策文件 944
進一步了解 946
AmazonNimbleStudio-StudioUser 946
使用此政策 946
政策詳細資訊 947
政策版本 947
JSON 政策文件 947
進一步了解 949
AmazonODBServiceRolePolicy 949
使用此政策 949
政策詳細資訊 949
政策版本 950
JSON 政策文件 950
進一步了解 951
AmazonOmicsFullAccess 951
使用此政策 952
政策詳細資訊 952
政策版本 952
JSON 政策文件 952
進一步了解 953
AmazonOmicsReadOnlyAccess 953
使用此政策 953
政策詳細資訊 953
政策版本 954
JSON 政策文件 954
進一步了解 954

AmazonOneEnterpriseFullAccess 954
使用此政策 955
政策詳細資訊 955
政策版本 955
JSON 政策文件 955
進一步了解 955
AmazonOneEnterpriseInstallerAccess 956
使用此政策 956
政策詳細資訊 956
政策版本 956
JSON 政策文件 956
進一步了解 957
AmazonOneEnterpriseReadOnlyAccess 957
使用此政策 957
政策詳細資訊 957
政策版本 957
JSON 政策文件 958
進一步了解 958
AmazonOpenSearchDashboardsServiceRolePolicy 958
使用此政策 958
政策詳細資訊 959
政策版本 959
JSON 政策文件 959
進一步了解 959
AmazonOpenSearchDirectQueryGlueCreateAccess 960
使用此政策 960
政策詳細資訊 960
政策版本 960
JSON 政策文件 960
進一步了解 961
AmazonOpenSearchIngestionFullAccess 961
使用此政策 961
政策詳細資訊 961
政策版本 961
JSON 政策文件 961
進一步了解 962

AmazonOpenSearchIngestionReadOnlyAccess 963
使用此政策 963
政策詳細資訊 963
政策版本 963
JSON 政策文件 963
進一步了解 964
AmazonOpenSearchIngestionServiceRolePolicy 964
使用此政策 964
政策詳細資訊 964
政策版本 964
JSON 政策文件 965
進一步了解 966
AmazonOpenSearchServerlessServiceRolePolicy 967
使用此政策 967
政策詳細資訊 967
政策版本 967
JSON 政策文件 967
進一步了解 968
AmazonOpenSearchServiceCognitoAccess 968
使用此政策 968
政策詳細資訊 968
政策版本 968
JSON 政策文件 968
進一步了解 970
AmazonOpenSearchServiceFullAccess 970
使用此政策 970
政策詳細資訊 970
政策版本 970
JSON 政策文件 970
進一步了解 971
AmazonOpenSearchServiceReadOnlyAccess 971
使用此政策 971
政策詳細資訊 971
政策版本 971
JSON 政策文件 972
進一步了解 972

AmazonOpenSearchServiceRolePolicy 972
使用此政策 972
政策詳細資訊 972
政策版本 973
JSON 政策文件 973
進一步了解 978
AmazonPersonalizeFullAccess 978
使用此政策 978
政策詳細資訊 978
政策版本 978
JSON 政策文件 978
進一步了解 980
AmazonPollyFullAccess 980
使用此政策 980
政策詳細資訊 980
政策版本 980
JSON 政策文件 980
進一步了解 981
AmazonPollyReadOnlyAccess 981
使用此政策 981
政策詳細資訊 981
政策版本 981
JSON 政策文件 982
進一步了解 982
AmazonPrometheusConsoleFullAccess 982
使用此政策 983
政策詳細資訊 983
政策版本 983
JSON 政策文件 983
進一步了解 984
AmazonPrometheusFullAccess 984
使用此政策 985
政策詳細資訊 985
政策版本 985
JSON 政策文件 985
進一步了解 986

AmazonPrometheusQueryAccess 986
使用此政策 986
政策詳細資訊 987
政策版本 987
JSON 政策文件 987
進一步了解 987
AmazonPrometheusRemoteWriteAccess 988
使用此政策 988
政策詳細資訊 988
政策版本 988
JSON 政策文件 988
進一步了解 989
AmazonPrometheusScraperServiceRolePolicy 989
使用此政策 989
政策詳細資訊 989
政策版本 989
JSON 政策文件 989
進一步了解 992
AmazonQDeveloperAccess 992
使用此政策 992
政策詳細資訊 992
政策版本 992
JSON 政策文件 992
進一步了解 994
AmazonQFullAccess 994
使用此政策 994
政策詳細資訊 994
政策版本 994
JSON 政策文件 994
進一步了解 996
AmazonQLDBConsoleFullAccess 996
使用此政策 996
政策詳細資訊 997
政策版本 997
JSON 政策文件 997
進一步了解 999

AmazonQLDBFullAccess 999
使用此政策 999
政策詳細資訊 999
政策版本 999
JSON 政策文件 999
進一步了解 1001
AmazonQLDBReadOnly 1001
使用此政策 1001
政策詳細資訊 1001
政策版本 1001
JSON 政策文件 1002
進一步了解 1002
AmazonRDSBetaServiceRolePolicy 1002
使用此政策 1003
政策詳細資訊 1003
政策版本 1003
JSON 政策文件 1003
進一步了解 1006
AmazonRDSCustomInstanceProfileRolePolicy 1006
使用此政策 1006
政策詳細資訊 1006
政策版本 1007
JSON 政策文件 1007
進一步了解 1014
AmazonRDSCustomPreviewServiceRolePolicy 1014
使用此政策 1014
政策詳細資訊 1014
政策版本 1015
JSON 政策文件 1015
進一步了解 1032
AmazonRDSCustomServiceRolePolicy 1032
使用此政策 1033
政策詳細資訊 1033
政策版本 1033
JSON 政策文件 1033
進一步了解 1052

AmazonRDSDataFullAccess 1052
使用此政策 1052
政策詳細資訊 1052
政策版本 1053
JSON 政策文件 1053
進一步了解 1054
AmazonRDSDirectoryServiceAccess 1054
使用此政策 1054
政策詳細資訊 1054
政策版本 1055
JSON 政策文件 1055
進一步了解 1055
AmazonRDSEnhancedMonitoringRole 1055
使用此政策 1056
政策詳細資訊 1056
政策版本 1056
JSON 政策文件 1056
進一步了解 1057
AmazonRDSFullAccess 1057
使用此政策 1057
政策詳細資訊 1057
政策版本 1057
JSON 政策文件 1058
進一步了解 1060
AmazonRDSPerformanceInsightsFullAccess 1060
使用此政策 1060
政策詳細資訊 1060
政策版本 1060
JSON 政策文件 1060
進一步了解 1062
AmazonRDSPerformanceInsightsReadOnly 1062
使用此政策 1062
政策詳細資訊 1062
政策版本 1063
JSON 政策文件 1063
進一步了解 1065

AmazonRDSPreviewServiceRolePolicy 1065
使用此政策 1065
政策詳細資訊 1065
政策版本 1066
JSON 政策文件 1066
進一步了解 1069
AmazonRDSReadOnlyAccess 1069
使用此政策 1069
政策詳細資訊 1069
政策版本 1069
JSON 政策文件 1069
進一步了解 1071
AmazonRDSServiceRolePolicy 1071
使用此政策 1071
政策詳細資訊 1071
政策版本 1071
JSON 政策文件 1072
進一步了解 1075
AmazonRedshiftAllCommandsFullAccess 1076
使用此政策 1076
政策詳細資訊 1076
政策版本 1076
JSON 政策文件 1076
進一步了解 1081
AmazonRedshiftDataFullAccess 1082
使用此政策 1082
政策詳細資訊 1082
政策版本 1082
JSON 政策文件 1082
進一步了解 1084
AmazonRedshiftFederatedAuthorization 1084
使用此政策 1085
政策詳細資訊 1085
政策版本 1085
JSON 政策文件 1085
進一步了解 1086

AmazonRedshiftFullAccess 1086
使用此政策 1086
政策詳細資訊 1087
政策版本 1087
JSON 政策文件 1087
進一步了解 1089
AmazonRedshiftQueryEditor 1089
使用此政策 1089
政策詳細資訊 1089
政策版本 1090
JSON 政策文件 1090
進一步了解 1092
AmazonRedshiftQueryEditorV2FullAccess 1092
使用此政策 1092
政策詳細資訊 1092
政策版本 1092
JSON 政策文件 1092
進一步了解 1094
AmazonRedshiftQueryEditorV2NoSharing 1094
使用此政策 1094
政策詳細資訊 1094
政策版本 1094
JSON 政策文件 1095
進一步了解 1098
AmazonRedshiftQueryEditorV2ReadSharing 1098
使用此政策 1099
政策詳細資訊 1099
政策版本 1099
JSON 政策文件 1099
進一步了解 1104
AmazonRedshiftQueryEditorV2ReadWriteSharing 1104
使用此政策 1104
政策詳細資訊 1104
政策版本 1105
JSON 政策文件 1105
進一步了解 1110

AmazonRedshiftReadOnlyAccess 1110
使用此政策 1110
政策詳細資訊 1110
政策版本 1110
JSON 政策文件 1111
進一步了解 1111
AmazonRedshiftServiceLinkedRolePolicy 1112
使用此政策 1112
政策詳細資訊 1112
政策版本 1112
JSON 政策文件 1112
進一步了解 1118
AmazonRekognitionCustomLabelsFullAccess 1119
使用此政策 1119
政策詳細資訊 1119
政策版本 1119
JSON 政策文件 1119
進一步了解 1120
AmazonRekognitionFullAccess 1121
使用此政策 1121
政策詳細資訊 1121
政策版本 1121
JSON 政策文件 1121
進一步了解 1122
AmazonRekognitionReadOnlyAccess 1122
使用此政策 1122
政策詳細資訊 1122
政策版本 1122
JSON 政策文件 1123
進一步了解 1124
AmazonRekognitionServiceRole 1124
使用此政策 1124
政策詳細資訊 1124
政策版本 1124
JSON 政策文件 1125
進一步了解 1125

AmazonRoute53AutoNamingFullAccess 1126
使用此政策 1126
政策詳細資訊 1126
政策版本 1126
JSON 政策文件 1126
進一步了解 1127
AmazonRoute53AutoNamingReadOnlyAccess 1127
使用此政策 1127
政策詳細資訊 1127
政策版本 1128
JSON 政策文件 1128
進一步了解 1128
AmazonRoute53AutoNamingRegistrantAccess 1128
使用此政策 1129
政策詳細資訊 1129
政策版本 1129
JSON 政策文件 1129
進一步了解 1130
AmazonRoute53DomainsFullAccess 1130
使用此政策 1130
政策詳細資訊 1130
政策版本 1130
JSON 政策文件 1131
進一步了解 1131
AmazonRoute53DomainsReadOnlyAccess 1131
使用此政策 1131
政策詳細資訊 1131
政策版本 1132
JSON 政策文件 1132
進一步了解 1132
AmazonRoute53FullAccess 1132
使用此政策 1133
政策詳細資訊 1133
政策版本 1133
JSON 政策文件 1133
進一步了解 1134

AmazonRoute53GlobalResolverFullAccess 1134
使用此政策 1134
政策詳細資訊 1135
政策版本 1135
JSON 政策文件 1135
進一步了解 1136
AmazonRoute53GlobalResolverReadOnlyAccess 1137
使用此政策 1137
政策詳細資訊 1137
政策版本 1137
JSON 政策文件 1137
進一步了解 1138
AmazonRoute53ProfilesFullAccess 1138
使用此政策 1138
政策詳細資訊 1138
政策版本 1139
JSON 政策文件 1139
進一步了解 1140
AmazonRoute53ProfilesReadOnlyAccess 1140
使用此政策 1140
政策詳細資訊 1140
政策版本 1141
JSON 政策文件 1141
進一步了解 1141
AmazonRoute53ReadOnlyAccess 1142
使用此政策 1142
政策詳細資訊 1142
政策版本 1142
JSON 政策文件 1142
進一步了解 1143
AmazonRoute53RecoveryClusterFullAccess 1143
使用此政策 1143
政策詳細資訊 1143
政策版本 1143
JSON 政策文件 1144
進一步了解 1144

AmazonRoute53RecoveryClusterReadOnlyAccess 1144
使用此政策 1144
政策詳細資訊 1144
政策版本 1145
JSON 政策文件 1145
進一步了解 1145
AmazonRoute53RecoveryControlConfigFullAccess 1145
使用此政策 1146
政策詳細資訊 1146
政策版本 1146
JSON 政策文件 1146
進一步了解 1146
AmazonRoute53RecoveryControlConfigReadOnlyAccess 1147
使用此政策 1147
政策詳細資訊 1147
政策版本 1147
JSON 政策文件 1147
進一步了解 1148
AmazonRoute53RecoveryReadinessFullAccess 1148
使用此政策 1148
政策詳細資訊 1148
政策版本 1149
JSON 政策文件 1149
進一步了解 1149
AmazonRoute53RecoveryReadinessReadOnlyAccess 1149
使用此政策 1150
政策詳細資訊 1150
政策版本 1150
JSON 政策文件 1150
進一步了解 1151
AmazonRoute53ResolverFullAccess 1151
使用此政策 1151
政策詳細資訊 1151
政策版本 1152
JSON 政策文件 1152
進一步了解 1152

AmazonRoute53ResolverReadOnlyAccess 1153
使用此政策 1153
政策詳細資訊 1153
政策版本 1153
JSON 政策文件 1153
進一步了解 1154
AmazonS3FullAccess 1154
使用此政策 1154
政策詳細資訊 1154
政策版本 1154
JSON 政策文件 1155
進一步了解 1155
AmazonS3ObjectLambdaExecutionRolePolicy 1155
使用此政策 1155
政策詳細資訊 1155
政策版本 1156
JSON 政策文件 1156
進一步了解 1156
AmazonS3OutpostsFullAccess 1156
使用此政策 1157
政策詳細資訊 1157
政策版本 1157
JSON 政策文件 1157
進一步了解 1158
AmazonS3OutpostsReadOnlyAccess 1158
使用此政策 1158
政策詳細資訊 1158
政策版本 1159
JSON 政策文件 1159
進一步了解 1160
AmazonS3ReadOnlyAccess 1160
使用此政策 1160
政策詳細資訊 1160
政策版本 1161
JSON 政策文件 1161
進一步了解 1161

AmazonS3TablesFullAccess 1161
使用此政策 1162
政策詳細資訊 1162
政策版本 1162
JSON 政策文件 1162
進一步了解 1163
AmazonS3TablesLakeFormationServiceRole 1163
使用此政策 1163
政策詳細資訊 1163
政策版本 1163
JSON 政策文件 1164
進一步了解 1166
AmazonS3TablesReadOnlyAccess 1166
使用此政策 1166
政策詳細資訊 1166
政策版本 1166
JSON 政策文件 1167
進一步了解 1167
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 1167
使用此政策 1167
政策詳細資訊 1168
政策版本 1168
JSON 政策文件 1168
進一步了解 1179
AmazonSageMakerCanvasAIServicesAccess 1180
使用此政策 1180
政策詳細資訊 1180
政策版本 1180
JSON 政策文件 1180
進一步了解 1183
AmazonSageMakerCanvasBedrockAccess 1183
使用此政策 1184
政策詳細資訊 1184
政策版本 1184
JSON 政策文件 1184
進一步了解 1185

AmazonSageMakerCanvasDataPrepFullAccess 1185
使用此政策 1185
政策詳細資訊 1185
政策版本 1186
JSON 政策文件 1186
進一步了解 1195
AmazonSageMakerCanvasDirectDeployAccess 1195
使用此政策 1195
政策詳細資訊 1196
政策版本 1196
JSON 政策文件 1196
進一步了解 1197
AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy 1197
使用此政策 1197
政策詳細資訊 1197
政策版本 1197
JSON 政策文件 1198
進一步了解 1199
AmazonSageMakerCanvasForecastAccess 1199
使用此政策 1199
政策詳細資訊 1199
政策版本 1200
JSON 政策文件 1200
進一步了解 1200
AmazonSageMakerCanvasFullAccess 1201
使用此政策 1201
政策詳細資訊 1201
政策版本 1201
JSON 政策文件 1201
進一步了解 1213
AmazonSageMakerCanvasSMDataScienceAssistantAccess 1214
使用此政策 1214
政策詳細資訊 1214
政策版本 1214
JSON 政策文件 1214
進一步了解 1215

AmazonSageMakerClusterInstanceRolePolicy 1215
使用此政策 1216
政策詳細資訊 1216
政策版本 1216
JSON 政策文件 1216
進一步了解 1218
AmazonSageMakerCoreServiceRolePolicy 1218
使用此政策 1218
政策詳細資訊 1218
政策版本 1218
JSON 政策文件 1219
進一步了解 1220
AmazonSageMakerEdgeDeviceFleetPolicy 1220
使用此政策 1220
政策詳細資訊 1220
政策版本 1220
JSON 政策文件 1220
進一步了解 1222
AmazonSageMakerFeatureStoreAccess 1222
使用此政策 1222
政策詳細資訊 1223
政策版本 1223
JSON 政策文件 1223
進一步了解 1224
AmazonSageMakerFullAccess 1224
使用此政策 1224
政策詳細資訊 1224
政策版本 1225
JSON 政策文件 1225
進一步了解 1241
AmazonSageMakerGeospatialExecutionRole 1241
使用此政策 1241
政策詳細資訊 1242
政策版本 1242
JSON 政策文件 1242
進一步了解 1243

AmazonSageMakerGeospatialFullAccess 1243
使用此政策 1243
政策詳細資訊 1243
政策版本 1243
JSON 政策文件 1244
進一步了解 1244
AmazonSageMakerGroundTruthExecution 1244
使用此政策 1245
政策詳細資訊 1245
政策版本 1245
JSON 政策文件 1245
進一步了解 1249
AmazonSageMakerHyperPodGatedModelAccess 1249
使用此政策 1249
政策詳細資訊 1249
政策版本 1249
JSON 政策文件 1249
進一步了解 1250
AmazonSageMakerHyperPodInferenceAccess 1250
使用此政策 1250
政策詳細資訊 1250
政策版本 1251
JSON 政策文件 1251
進一步了解 1258
AmazonSageMakerHyperPodObservabilityAdminAccess 1259
使用此政策 1259
政策詳細資訊 1259
政策版本 1259
JSON 政策文件 1259
進一步了解 1266
AmazonSageMakerHyperPodServiceRolePolicy 1266
使用此政策 1266
政策詳細資訊 1266
政策版本 1266
JSON 政策文件 1266
進一步了解 1268

AmazonSageMakerHyperPodTrainingOperatorAccess 1268
使用此政策 1268
政策詳細資訊 1268
政策版本 1268
JSON 政策文件 1268
進一步了解 1269
AmazonSageMakerMechanicalTurkAccess 1269
使用此政策 1269
政策詳細資訊 1269
政策版本 1270
JSON 政策文件 1270
進一步了解 1270
AmazonSageMakerModelGovernanceUseAccess 1270
使用此政策 1270
政策詳細資訊 1271
政策版本 1271
JSON 政策文件 1271
進一步了解 1273
AmazonSageMakerModelRegistryFullAccess 1273
使用此政策 1273
政策詳細資訊 1273
政策版本 1273
JSON 政策文件 1274
進一步了解 1277
AmazonSageMakerNotebooksServiceRolePolicy 1277
使用此政策 1278
政策詳細資訊 1278
政策版本 1278
JSON 政策文件 1278
進一步了解 1283
AmazonSageMakerPartnerAppsFullAccess 1283
使用此政策 1284
政策詳細資訊 1284
政策版本 1284
JSON 政策文件 1284
進一步了解 1285

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 1285
使用此政策 1285
政策詳細資訊 1285
政策版本 1286
JSON 政策文件 1286
進一步了解 1287
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 1287
使用此政策 1287
政策詳細資訊 1287
政策版本 1287
JSON 政策文件 1288
進一步了解 1291
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1291
使用此政策 1291
政策詳細資訊 1292
政策版本 1292
JSON 政策文件 1292
進一步了解 1292
AmazonSageMakerPipelinesIntegrations 1293
使用此政策 1293
政策詳細資訊 1293
政策版本 1293
JSON 政策文件 1293
進一步了解 1295
AmazonSageMakerQuickSightVPCPolicy 1295
使用此政策 1296
政策詳細資訊 1296
政策版本 1296
JSON 政策文件 1296
進一步了解 1298
AmazonSageMakerReadOnly 1298
使用此政策 1298
政策詳細資訊 1298
政策版本 1298
JSON 政策文件 1298
進一步了解 1300

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1300
使用此政策 1300
政策詳細資訊 1300
政策版本 1300
JSON 政策文件 1301
進一步了解 1301
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1302
使用此政策 1302
政策詳細資訊 1302
政策版本 1302
JSON 政策文件 1302
進一步了解 1309
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1309
使用此政策 1309
政策詳細資訊 1310
政策版本 1310
JSON 政策文件 1310
進一步了解 1320
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1320
使用此政策 1321
政策詳細資訊 1321
政策版本 1321
JSON 政策文件 1321
進一步了解 1324
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1324
使用此政策 1324
政策詳細資訊 1324
政策版本 1325
JSON 政策文件 1325
進一步了解 1325
AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1325
使用此政策 1326
政策詳細資訊 1326
政策版本 1326
JSON 政策文件 1326
進一步了解 1326

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1327
使用此政策 1327
政策詳細資訊 1327
政策版本 1327
JSON 政策文件 1327
進一步了解 1330
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1330
使用此政策 1330
政策詳細資訊 1330
政策版本 1330
JSON 政策文件 1331
進一步了解 1341
AmazonSageMakerSpacesControllerPolicy 1341
使用此政策 1341
政策詳細資訊 1341
政策版本 1341
JSON 政策文件 1341
進一步了解 1346
AmazonSageMakerSpacesRouterPolicy 1346
使用此政策 1346
政策詳細資訊 1346
政策版本 1347
JSON 政策文件 1347
進一步了解 1348
AmazonSageMakerTrainingPlanCreateAccess 1348
使用此政策 1348
政策詳細資訊 1348
政策版本 1348
JSON 政策文件 1348
進一步了解 1350
AmazonSecurityLakeAdministrator 1350
使用此政策 1350
政策詳細資訊 1350
政策版本 1351
JSON 政策文件 1351
進一步了解 1362

AmazonSecurityLakeMetastoreManager 1362
使用此政策 1362
政策詳細資訊 1362
政策版本 1363
JSON 政策文件 1363
進一步了解 1365
AmazonSecurityLakePermissionsBoundary 1365
使用此政策 1365
政策詳細資訊 1365
政策版本 1366
JSON 政策文件 1366
進一步了解 1369
AmazonSESFullAccess 1369
使用此政策 1369
政策詳細資訊 1369
政策版本 1370
JSON 政策文件 1370
進一步了解 1370
AmazonSESReadOnlyAccess 1370
使用此政策 1370
政策詳細資訊 1371
政策版本 1371
JSON 政策文件 1371
進一步了解 1371
AmazonSESServiceRolePolicy 1372
使用此政策 1372
政策詳細資訊 1372
政策版本 1372
JSON 政策文件 1372
進一步了解 1373
AmazonSNSFullAccess 1373
使用此政策 1373
政策詳細資訊 1373
政策版本 1373
JSON 政策文件 1374
進一步了解 1374

AmazonSNSReadOnlyAccess 1375
使用此政策 1375
政策詳細資訊 1375
政策版本 1375
JSON 政策文件 1375
進一步了解 1376
AmazonSNSRole 1376
使用此政策 1377
政策詳細資訊 1377
政策版本 1377
JSON 政策文件 1377
進一步了解 1378
AmazonSQSFullAccess 1378
使用此政策 1378
政策詳細資訊 1378
政策版本 1378
JSON 政策文件 1378
進一步了解 1379
AmazonSQSReadOnlyAccess 1379
使用此政策 1379
政策詳細資訊 1379
政策版本 1379
JSON 政策文件 1380
進一步了解 1380
AmazonSSMAutomationApproverAccess 1380
使用此政策 1380
政策詳細資訊 1381
政策版本 1381
JSON 政策文件 1381
進一步了解 1381
AmazonSSMAutomationRole 1382
使用此政策 1382
政策詳細資訊 1382
政策版本 1382
JSON 政策文件 1382
進一步了解 1384

AmazonSSMDirectoryServiceAccess 1384
使用此政策 1384
政策詳細資訊 1384
政策版本 1385
JSON 政策文件 1385
進一步了解 1385
AmazonSSMFullAccess 1385
使用此政策 1385
政策詳細資訊 1386
政策版本 1386
JSON 政策文件 1386
進一步了解 1387
AmazonSSMMaintenanceWindowRole 1387
使用此政策 1387
政策詳細資訊 1388
政策版本 1388
JSON 政策文件 1388
進一步了解 1389
AmazonSSMManagedEC2InstanceDefaultPolicy 1390
使用此政策 1390
政策詳細資訊 1390
政策版本 1390
JSON 政策文件 1390
進一步了解 1391
AmazonSSMManagedInstanceCore 1392
使用此政策 1392
政策詳細資訊 1392
政策版本 1392
JSON 政策文件 1392
進一步了解 1393
AmazonSSMPatchAssociation 1394
使用此政策 1394
政策詳細資訊 1394
政策版本 1394
JSON 政策文件 1394
進一步了解 1395

AmazonSSMReadOnlyAccess 1395
使用此政策 1395
政策詳細資訊 1395
政策版本 1396
JSON 政策文件 1396
進一步了解 1396
AmazonSSMServiceRolePolicy 1396
使用此政策 1397
政策詳細資訊 1397
政策版本 1397
JSON 政策文件 1397
進一步了解 1403
AmazonSumerianFullAccess 1403
使用此政策 1403
政策詳細資訊 1403
政策版本 1403
JSON 政策文件 1403
進一步了解 1404
AmazonTextractFullAccess 1404
使用此政策 1404
政策詳細資訊 1404
政策版本 1404
JSON 政策文件 1405
進一步了解 1405
AmazonTextractServiceRole 1405
使用此政策 1405
政策詳細資訊 1405
政策版本 1406
JSON 政策文件 1406
進一步了解 1406
AmazonTimestreamConsoleFullAccess 1406
使用此政策 1407
政策詳細資訊 1407
政策版本 1407
JSON 政策文件 1407
進一步了解 1410

AmazonTimestreamFullAccess 1410
使用此政策 1410
政策詳細資訊 1410
政策版本 1410
JSON 政策文件 1411
進一步了解 1412
AmazonTimestreamInfluxDBFullAccess 1412
使用此政策 1412
政策詳細資訊 1412
政策版本 1412
JSON 政策文件 1413
進一步了解 1415
AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 1415
使用此政策 1415
政策詳細資訊 1416
政策版本 1416
JSON 政策文件 1416
進一步了解 1418
AmazonTimestreamInfluxDBServiceRolePolicy 1418
使用此政策 1418
政策詳細資訊 1419
政策版本 1419
JSON 政策文件 1419
進一步了解 1421
AmazonTimestreamReadOnlyAccess 1422
使用此政策 1422
政策詳細資訊 1422
政策版本 1422
JSON 政策文件 1422
進一步了解 1423
AmazonTranscribeFullAccess 1423
使用此政策 1423
政策詳細資訊 1423
政策版本 1424
JSON 政策文件 1424
進一步了解 1424

AmazonTranscribeReadOnlyAccess 1425
使用此政策 1425
政策詳細資訊 1425
政策版本 1425
JSON 政策文件 1425
進一步了解 1426
AmazonVerifiedPermissionsFullAccess 1426
使用此政策 1426
政策詳細資訊 1426
政策版本 1426
JSON 政策文件 1427
進一步了解 1427
AmazonVerifiedPermissionsReadOnlyAccess 1427
使用此政策 1428
政策詳細資訊 1428
政策版本 1428
JSON 政策文件 1428
進一步了解 1429
AmazonVPCCrossAccountNetworkInterfaceOperations 1429
使用此政策 1429
政策詳細資訊 1429
政策版本 1430
JSON 政策文件 1430
進一步了解 1431
AmazonVPCFullAccess 1431
使用此政策 1431
政策詳細資訊 1432
政策版本 1432
JSON 政策文件 1432
進一步了解 1436
AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1436
使用此政策 1436
政策詳細資訊 1436
政策版本 1437
JSON 政策文件 1437
進一步了解 1440

AmazonVPCReachabilityAnalyzerFullAccessPolicy 1440
使用此政策 1440
政策詳細資訊 1441
政策版本 1441
JSON 政策文件 1441
進一步了解 1444
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1444
使用此政策 1444
政策詳細資訊 1444
政策版本 1445
JSON 政策文件 1445
進一步了解 1445
AmazonVPCReadOnlyAccess 1446
使用此政策 1446
政策詳細資訊 1446
政策版本 1446
JSON 政策文件 1446
進一步了解 1447
AmazonWorkDocsFullAccess 1448
使用此政策 1448
政策詳細資訊 1448
政策版本 1448
JSON 政策文件 1448
進一步了解 1449
AmazonWorkDocsReadOnlyAccess 1449
使用此政策 1449
政策詳細資訊 1449
政策版本 1449
JSON 政策文件 1450
進一步了解 1450
AmazonWorkMailEventsServiceRolePolicy 1450
使用此政策 1450
政策詳細資訊 1450
政策版本 1451
JSON 政策文件 1451
進一步了解 1451

AmazonWorkMailFullAccess 1451
使用此政策 1452
政策詳細資訊 1452
政策版本 1452
JSON 政策文件 1452
進一步了解 1454
AmazonWorkMailMessageFlowFullAccess 1454
使用此政策 1454
政策詳細資訊 1454
政策版本 1455
JSON 政策文件 1455
進一步了解 1455
AmazonWorkMailMessageFlowReadOnlyAccess 1455
使用此政策 1456
政策詳細資訊 1456
政策版本 1456
JSON 政策文件 1456
進一步了解 1456
AmazonWorkMailReadOnlyAccess 1457
使用此政策 1457
政策詳細資訊 1457
政策版本 1457
JSON 政策文件 1457
進一步了解 1458
AmazonWorkSpacesAdmin 1458
使用此政策 1458
政策詳細資訊 1458
政策版本 1459
JSON 政策文件 1459
進一步了解 1460
AmazonWorkSpacesApplicationManagerAdminAccess 1460
使用此政策 1460
政策詳細資訊 1460
政策版本 1461
JSON 政策文件 1461
進一步了解 1461

AmazonWorkspacesPCAAccess 1461
使用此政策 1461
政策詳細資訊 1462
政策版本 1462
JSON 政策文件 1462
進一步了解 1462
AmazonWorkSpacesPoolServiceAccess 1463
使用此政策 1463
政策詳細資訊 1463
政策版本 1463
JSON 政策文件 1463
進一步了解 1465
AmazonWorkSpacesSecureBrowserReadOnly 1465
使用此政策 1465
政策詳細資訊 1465
政策版本 1465
JSON 政策文件 1465
進一步了解 1466
AmazonWorkSpacesSelfServiceAccess 1467
使用此政策 1467
政策詳細資訊 1467
政策版本 1467
JSON 政策文件 1467
進一步了解 1468
AmazonWorkSpacesServiceAccess 1468
使用此政策 1468
政策詳細資訊 1468
政策版本 1468
JSON 政策文件 1469
進一步了解 1469
AmazonWorkSpacesThinClientFullAccess 1469
使用此政策 1469
政策詳細資訊 1469
政策版本 1470
JSON 政策文件 1470
進一步了解 1471

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 1471
使用此政策 1471
政策詳細資訊 1472
政策版本 1472
JSON 政策文件 1472
進一步了解 1473
AmazonWorkSpacesThinClientReadOnlyAccess 1473
使用此政策 1473
政策詳細資訊 1473
政策版本 1473
JSON 政策文件 1473
進一步了解 1475
AmazonWorkSpacesWebReadOnly 1475
使用此政策 1475
政策詳細資訊 1475
政策版本 1475
JSON 政策文件 1475
進一步了解 1476
AmazonWorkSpacesWebServiceRolePolicy 1477
使用此政策 1477
政策詳細資訊 1477
政策版本 1477
JSON 政策文件 1477
進一步了解 1479
AmazonZocaloFullAccess 1480
使用此政策 1480
政策詳細資訊 1480
政策版本 1480
JSON 政策文件 1480
進一步了解 1481
AmazonZocaloReadOnlyAccess 1481
使用此政策 1481
政策詳細資訊 1481
政策版本 1482
JSON 政策文件 1482
進一步了解 1482

AmplifyBackendDeployFullAccess 1482
使用此政策 1483
政策詳細資訊 1483
政策版本 1483
JSON 政策文件 1483
進一步了解 1487
APIGatewayServiceRolePolicy 1488
使用此政策 1488
政策詳細資訊 1488
政策版本 1488
JSON 政策文件 1488
進一步了解 1490
AppIntegrationsServiceLinkedRolePolicy 1491
使用此政策 1491
政策詳細資訊 1491
政策版本 1491
JSON 政策文件 1491
進一步了解 1493
ApplicationAutoScalingForAmazonAppStreamAccess 1493
使用此政策 1493
政策詳細資訊 1493
政策版本 1493
JSON 政策文件 1494
進一步了解 1494
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1494
使用此政策 1495
政策詳細資訊 1495
政策版本 1495
JSON 政策文件 1495
進一步了解 1497
AppRunnerNetworkingServiceRolePolicy 1497
使用此政策 1497
政策詳細資訊 1497
政策版本 1498
JSON 政策文件 1498
進一步了解 1499

AppRunnerServiceRolePolicy 1499
使用此政策 1499
政策詳細資訊 1499
政策版本 1500
JSON 政策文件 1500
進一步了解 1501
AppStudioServiceRolePolicy 1501
使用此政策 1501
政策詳細資訊 1501
政策版本 1501
JSON 政策文件 1502
進一步了解 1504
AuroraDsqlServiceLinkedRolePolicy 1504
使用此政策 1504
政策詳細資訊 1504
政策版本 1504
JSON 政策文件 1505
進一步了解 1505
AutoScalingConsoleFullAccess 1505
使用此政策 1505
政策詳細資訊 1506
政策版本 1506
JSON 政策文件 1506
進一步了解 1508
AutoScalingConsoleReadOnlyAccess 1508
使用此政策 1508
政策詳細資訊 1508
政策版本 1508
JSON 政策文件 1508
進一步了解 1510
AutoScalingFullAccess 1510
使用此政策 1510
政策詳細資訊 1510
政策版本 1510
JSON 政策文件 1510
進一步了解 1512

AutoScalingNotificationAccessRole 1512
使用此政策 1512
政策詳細資訊 1512
政策版本 1512
JSON 政策文件 1513
進一步了解 1513
AutoScalingReadOnlyAccess 1513
使用此政策 1513
政策詳細資訊 1513
政策版本 1514
JSON 政策文件 1514
進一步了解 1514
AutoScalingServiceRolePolicy 1514
使用此政策 1514
政策詳細資訊 1515
政策版本 1515
JSON 政策文件 1515
進一步了解 1518
AWS-SSM-Automation-DiagnosisBucketPolicy 1518
使用此政策 1518
政策詳細資訊 1518
政策版本 1519
JSON 政策文件 1519
進一步了解 1521
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 1521
使用此政策 1521
政策詳細資訊 1521
政策版本 1522
JSON 政策文件 1522
進一步了解 1524
AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 1525
使用此政策 1525
政策詳細資訊 1525
政策版本 1525
JSON 政策文件 1525
進一步了解 1527

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 1527
使用此政策 1528
政策詳細資訊 1528
政策版本 1528
JSON 政策文件 1528
進一步了解 1529
AWS-SSM-RemediationAutomation-AdministrationRolePolicy 1529
使用此政策 1529
政策詳細資訊 1529
政策版本 1530
JSON 政策文件 1530
進一步了解 1532
AWS-SSM-RemediationAutomation-ExecutionRolePolicy 1532
使用此政策 1533
政策詳細資訊 1533
政策版本 1533
JSON 政策文件 1533
進一步了解 1539
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 1540
使用此政策 1540
政策詳細資訊 1540
政策版本 1540
JSON 政策文件 1540
進一步了解 1541
AWS_ConfigRole 1541
使用此政策 1541
政策詳細資訊 1541
政策版本 1542
JSON 政策文件 1542
進一步了解 1592
AWSAccountActivityAccess 1592
使用此政策 1593
政策詳細資訊 1593
政策版本 1593
JSON 政策文件 1593
進一步了解 1594

AWSAccountManagementFullAccess 1594
使用此政策 1594
政策詳細資訊 1594
政策版本 1594
JSON 政策文件 1595
進一步了解 1595
AWSAccountManagementReadOnlyAccess 1595
使用此政策 1595
政策詳細資訊 1595
政策版本 1596
JSON 政策文件 1596
進一步了解 1596
AWSAccountSettingsManagementRole 1596
使用此政策 1596
政策詳細資訊 1597
政策版本 1597
JSON 政策文件 1597
進一步了解 1599
AWSAccountUsageReportAccess 1599
使用此政策 1600
政策詳細資訊 1600
政策版本 1600
JSON 政策文件 1600
進一步了解 1600
AWSAgentlessDiscoveryService 1601
使用此政策 1601
政策詳細資訊 1601
政策版本 1601
JSON 政策文件 1601
進一步了解 1603
AWSAppFabricFullAccess 1603
使用此政策 1603
政策詳細資訊 1604
政策版本 1604
JSON 政策文件 1604
進一步了解 1605

AWSAppFabricReadOnlyAccess 1605
使用此政策 1606
政策詳細資訊 1606
政策版本 1606
JSON 政策文件 1606
進一步了解 1607
AWSAppFabricServiceRolePolicy 1607
使用此政策 1607
政策詳細資訊 1607
政策版本 1607
JSON 政策文件 1607
進一步了解 1609
AWSApplicationAutoscalingAppStreamFleetPolicy 1609
使用此政策 1609
政策詳細資訊 1609
政策版本 1609
JSON 政策文件 1609
進一步了解 1610
AWSApplicationAutoscalingCassandraTablePolicy 1610
使用此政策 1610
政策詳細資訊 1610
政策版本 1611
JSON 政策文件 1611
進一步了解 1611
AWSApplicationAutoscalingComprehendEndpointPolicy 1612
使用此政策 1612
政策詳細資訊 1612
政策版本 1612
JSON 政策文件 1612
進一步了解 1613
AWSApplicationAutoScalingCustomResourcePolicy 1613
使用此政策 1613
政策詳細資訊 1613
政策版本 1613
JSON 政策文件 1614
進一步了解 1614

AWSApplicationAutoscalingDynamoDBTablePolicy 1614
使用此政策 1614
政策詳細資訊 1614
政策版本 1615
JSON 政策文件 1615
進一步了解 1615
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1615
使用此政策 1616
政策詳細資訊 1616
政策版本 1616
JSON 政策文件 1616
進一步了解 1617
AWSApplicationAutoscalingECSServicePolicy 1617
使用此政策 1617
政策詳細資訊 1617
政策版本 1617
JSON 政策文件 1617
進一步了解 1618
AWSApplicationAutoscalingElastiCacheRGPolicy 1618
使用此政策 1618
政策詳細資訊 1618
政策版本 1619
JSON 政策文件 1619
進一步了解 1620
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1620
使用此政策 1620
政策詳細資訊 1620
政策版本 1621
JSON 政策文件 1621
進一步了解 1621
AWSApplicationAutoscalingKafkaClusterPolicy 1621
使用此政策 1622
政策詳細資訊 1622
政策版本 1622
JSON 政策文件 1622
進一步了解 1623

AWSApplicationAutoscalingLambdaConcurrencyPolicy 1623
使用此政策 1623
政策詳細資訊 1623
政策版本 1623
JSON 政策文件 1623
進一步了解 1624
AWSApplicationAutoscalingNeptuneClusterPolicy 1624
使用此政策 1624
政策詳細資訊 1624
政策版本 1625
JSON 政策文件 1625
進一步了解 1626
AWSApplicationAutoscalingRDSClusterPolicy 1626
使用此政策 1627
政策詳細資訊 1627
政策版本 1627
JSON 政策文件 1627
進一步了解 1628
AWSApplicationAutoscalingSageMakerEndpointPolicy 1628
使用此政策 1628
政策詳細資訊 1628
政策版本 1629
JSON 政策文件 1629
進一步了解 1630
AWSApplicationAutoscalingWorkSpacesPoolPolicy 1630
使用此政策 1630
政策詳細資訊 1630
政策版本 1630
JSON 政策文件 1630
進一步了解 1632
AWSApplicationDiscoveryAgentAccess 1632
使用此政策 1632
政策詳細資訊 1632
政策版本 1632
JSON 政策文件 1633
進一步了解 1633

AWSApplicationDiscoveryAgentlessCollectorAccess 1633
使用此政策 1634
政策詳細資訊 1634
政策版本 1634
JSON 政策文件 1634
進一步了解 1635
AWSApplicationDiscoveryServiceFullAccess 1635
使用此政策 1635
政策詳細資訊 1636
政策版本 1636
JSON 政策文件 1636
進一步了解 1637
AWSApplicationMigrationAgentInstallationPolicy 1638
使用此政策 1638
政策詳細資訊 1638
政策版本 1638
JSON 政策文件 1638
進一步了解 1639
AWSApplicationMigrationAgentPolicy 1639
使用此政策 1640
政策詳細資訊 1640
政策版本 1640
JSON 政策文件 1640
進一步了解 1641
AWSApplicationMigrationAgentPolicy_v2 1641
使用此政策 1641
政策詳細資訊 1641
政策版本 1642
JSON 政策文件 1642
進一步了解 1642
AWSApplicationMigrationConversionServerPolicy 1643
使用此政策 1643
政策詳細資訊 1643
政策版本 1643
JSON 政策文件 1643
進一步了解 1644

AWSApplicationMigrationEC2Access 1644
使用此政策 1644
政策詳細資訊 1644
政策版本 1645
JSON 政策文件 1645
進一步了解 1653
AWSApplicationMigrationFullAccess 1653
使用此政策 1653
政策詳細資訊 1653
政策版本 1653
JSON 政策文件 1654
進一步了解 1660
AWSApplicationMigrationMGHAccess 1660
使用此政策 1660
政策詳細資訊 1660
政策版本 1660
JSON 政策文件 1661
進一步了解 1661
AWSApplicationMigrationNetworkMigrationCustomResource 1661
使用此政策 1661
政策詳細資訊 1662
政策版本 1662
JSON 政策文件 1662
進一步了解 1663
AWSApplicationMigrationNetworkMigrationMultiAccount 1663
使用此政策 1663
政策詳細資訊 1663
政策版本 1663
JSON 政策文件 1663
進一步了解 1688
AWSApplicationMigrationReadOnlyAccess 1688
使用此政策 1688
政策詳細資訊 1688
政策版本 1688
JSON 政策文件 1689
進一步了解 1690

AWSApplicationMigrationReplicationServerPolicy 1690
使用此政策 1690
政策詳細資訊 1690
政策版本 1691
JSON 政策文件 1691
進一步了解 1692
AWSApplicationMigrationServiceEc2InstancePolicy 1693
使用此政策 1693
政策詳細資訊 1693
政策版本 1693
JSON 政策文件 1693
進一步了解 1694
AWSApplicationMigrationServiceRolePolicy 1695
使用此政策 1695
政策詳細資訊 1695
政策版本 1695
JSON 政策文件 1695
進一步了解 1703
AWSApplicationMigrationSSMAccess 1703
使用此政策 1703
政策詳細資訊 1703
政策版本 1703
JSON 政策文件 1703
進一步了解 1705
AWSApplicationMigrationVCenterClientPolicy 1705
使用此政策 1706
政策詳細資訊 1706
政策版本 1706
JSON 政策文件 1706
進一步了解 1707
AWSAppMeshEnvoyAccess 1707
使用此政策 1707
政策詳細資訊 1707
政策版本 1707
JSON 政策文件 1708
進一步了解 1708

AWSAppMeshFullAccess 1708
使用此政策 1708
政策詳細資訊 1708
政策版本 1709
JSON 政策文件 1709
進一步了解 1710
AWSAppMeshPreviewEnvoyAccess 1710
使用此政策 1711
政策詳細資訊 1711
政策版本 1711
JSON 政策文件 1711
進一步了解 1711
AWSAppMeshPreviewServiceRolePolicy 1712
使用此政策 1712
政策詳細資訊 1712
政策版本 1712
JSON 政策文件 1712
進一步了解 1713
AWSAppMeshReadOnly 1713
使用此政策 1713
政策詳細資訊 1713
政策版本 1714
JSON 政策文件 1714
進一步了解 1715
AWSAppMeshServiceRolePolicy 1715
使用此政策 1715
政策詳細資訊 1715
政策版本 1715
JSON 政策文件 1716
進一步了解 1716
AWSAppRunnerFullAccess 1716
使用此政策 1716
政策詳細資訊 1717
政策版本 1717
JSON 政策文件 1717
進一步了解 1718

AWSAppRunnerReadOnlyAccess 1718
使用此政策 1718
政策詳細資訊 1718
政策版本 1718
JSON 政策文件 1719
進一步了解 1719
AWSAppRunnerServicePolicyForECRAccess 1719
使用此政策 1719
政策詳細資訊 1719
政策版本 1720
JSON 政策文件 1720
進一步了解 1720
AWSAppSyncAdministrator 1720
使用此政策 1721
政策詳細資訊 1721
政策版本 1721
JSON 政策文件 1721
進一步了解 1722
AWSAppSyncInvokeFullAccess 1722
使用此政策 1723
政策詳細資訊 1723
政策版本 1723
JSON 政策文件 1723
進一步了解 1723
AWSAppSyncPushToCloudWatchLogs 1724
使用此政策 1724
政策詳細資訊 1724
政策版本 1724
JSON 政策文件 1724
進一步了解 1725
AWSAppSyncSchemaAuthor 1725
使用此政策 1725
政策詳細資訊 1725
政策版本 1725
JSON 政策文件 1726
進一步了解 1727

AWSAppSyncServiceRolePolicy 1727
使用此政策 1727
政策詳細資訊 1727
政策版本 1727
JSON 政策文件 1727
進一步了解 1728
AWSArtifactAccountSync 1728
使用此政策 1728
政策詳細資訊 1728
政策版本 1728
JSON 政策文件 1729
進一步了解 1729
AWSArtifactAgreementsFullAccess 1729
使用此政策 1729
政策詳細資訊 1730
政策版本 1730
JSON 政策文件 1730
進一步了解 1732
AWSArtifactAgreementsReadOnlyAccess 1732
使用此政策 1732
政策詳細資訊 1732
政策版本 1733
JSON 政策文件 1733
進一步了解 1734
AWSArtifactReportsReadOnlyAccess 1734
使用此政策 1734
政策詳細資訊 1734
政策版本 1734
JSON 政策文件 1735
進一步了解 1735
AWSArtifactServiceRolePolicy 1735
使用此政策 1735
政策詳細資訊 1736
政策版本 1736
JSON 政策文件 1736
進一步了解 1736

AWSAuditManagerAdministratorAccess 1737
使用此政策 1737
政策詳細資訊 1737
政策版本 1737
JSON 政策文件 1737
進一步了解 1741
AWSAuditManagerServiceRolePolicy 1741
使用此政策 1742
政策詳細資訊 1742
政策版本 1742
JSON 政策文件 1742
進一步了解 1749
AWSAutoScalingPlansEC2AutoScalingPolicy 1749
使用此政策 1749
政策詳細資訊 1749
政策版本 1749
JSON 政策文件 1750
進一步了解 1750
AWSBackupAuditAccess 1750
使用此政策 1750
政策詳細資訊 1751
政策版本 1751
JSON 政策文件 1751
進一步了解 1752
AWSBackupDataTransferAccess 1752
使用此政策 1753
政策詳細資訊 1753
政策版本 1753
JSON 政策文件 1753
進一步了解 1754
AWSBackupFullAccess 1754
使用此政策 1754
政策詳細資訊 1754
政策版本 1754
JSON 政策文件 1754
進一步了解 1766

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 1766
使用此政策 1767
政策詳細資訊 1767
政策版本 1767
JSON 政策文件 1767
進一步了解 1768
AWSBackupGuardDutyRolePolicyForScans 1768
使用此政策 1768
政策詳細資訊 1768
政策版本 1768
JSON 政策文件 1769
進一步了解 1772
AWSBackupOperatorAccess 1773
使用此政策 1773
政策詳細資訊 1773
政策版本 1773
JSON 政策文件 1773
進一步了解 1782
AWSBackupOrganizationAdminAccess 1783
使用此政策 1783
政策詳細資訊 1783
政策版本 1783
JSON 政策文件 1783
進一步了解 1785
AWSBackupRestoreAccessForSAPHANA 1785
使用此政策 1785
政策詳細資訊 1785
政策版本 1786
JSON 政策文件 1786
進一步了解 1787
AWSBackupSearchOperatorAccess 1787
使用此政策 1787
政策詳細資訊 1787
政策版本 1787
JSON 政策文件 1788
進一步了解 1789

AWSBackupServiceLinkedRolePolicyForBackup 1789
使用此政策 1790
政策詳細資訊 1790
政策版本 1790
JSON 政策文件 1790
進一步了解 1800
AWSBackupServiceLinkedRolePolicyForBackupTest 1800
使用此政策 1801
政策詳細資訊 1801
政策版本 1801
JSON 政策文件 1801
進一步了解 1802
AWSBackupServiceRolePolicyForBackup 1802
使用此政策 1802
政策詳細資訊 1802
政策版本 1802
JSON 政策文件 1803
進一步了解 1817
AWSBackupServiceRolePolicyForIndexing 1817
使用此政策 1818
政策詳細資訊 1818
政策版本 1818
JSON 政策文件 1818
進一步了解 1819
AWSBackupServiceRolePolicyForItemRestores 1819
使用此政策 1819
政策詳細資訊 1820
政策版本 1820
JSON 政策文件 1820
進一步了解 1822
AWSBackupServiceRolePolicyForRestores 1822
使用此政策 1822
政策詳細資訊 1822
政策版本 1822
JSON 政策文件 1823
進一步了解 1836

AWSBackupServiceRolePolicyForS3Backup 1837
使用此政策 1837
政策詳細資訊 1837
政策版本 1837
JSON 政策文件 1837
進一步了解 1840
AWSBackupServiceRolePolicyForS3Restore 1840
使用此政策 1840
政策詳細資訊 1840
政策版本 1840
JSON 政策文件 1840
進一步了解 1842
AWSBackupServiceRolePolicyForScans 1842
使用此政策 1842
政策詳細資訊 1842
政策版本 1842
JSON 政策文件 1843
進一步了解 1843
AWSBatchFullAccess 1844
使用此政策 1844
政策詳細資訊 1844
政策版本 1844
JSON 政策文件 1844
進一步了解 1846
AWSBatchServiceEventTargetRole 1846
使用此政策 1846
政策詳細資訊 1846
政策版本 1846
JSON 政策文件 1846
進一步了解 1847
AWSBatchServiceRole 1847
使用此政策 1847
政策詳細資訊 1847
政策版本 1848
JSON 政策文件 1848
進一步了解 1851

AWSBatchServiceRolePolicyForSageMaker 1851
使用此政策 1851
政策詳細資訊 1851
政策版本 1852
JSON 政策文件 1852
進一步了解 1853
AWSBCMDataExportsServiceRolePolicy 1853
使用此政策 1853
政策詳細資訊 1854
政策版本 1854
JSON 政策文件 1854
進一步了解 1854
AWSBillingConductorFullAccess 1855
使用此政策 1855
政策詳細資訊 1855
政策版本 1855
JSON 政策文件 1855
進一步了解 1856
AWSBillingConductorReadOnlyAccess 1856
使用此政策 1856
政策詳細資訊 1856
政策版本 1857
JSON 政策文件 1857
進一步了解 1857
AWSBillingReadOnlyAccess 1858
使用此政策 1858
政策詳細資訊 1858
政策版本 1858
JSON 政策文件 1858
進一步了解 1860
AWSBillingServiceRolePolicy 1860
使用此政策 1861
政策詳細資訊 1861
政策版本 1861
JSON 政策文件 1861
進一步了解 1861

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 1862
使用此政策 1862
政策詳細資訊 1862
政策版本 1862
JSON 政策文件 1862
進一步了解 1863
AWSBudgetsActionsWithAWSResourceControlAccess 1863
使用此政策 1864
政策詳細資訊 1864
政策版本 1864
JSON 政策文件 1864
進一步了解 1865
AWSBudgetsReadOnlyAccess 1866
使用此政策 1866
政策詳細資訊 1866
政策版本 1866
JSON 政策文件 1866
進一步了解 1867
AWSBugBustFullAccess 1867
使用此政策 1867
政策詳細資訊 1867
政策版本 1867
JSON 政策文件 1868
進一步了解 1869
AWSBugBustPlayerAccess 1869
使用此政策 1869
政策詳細資訊 1869
政策版本 1869
JSON 政策文件 1869
進一步了解 1870
AWSBugBustServiceRolePolicy 1871
使用此政策 1871
政策詳細資訊 1871
政策版本 1871
JSON 政策文件 1871
進一步了解 1872

AWSCertificateManagerFullAccess 1872
使用此政策 1872
政策詳細資訊 1872
政策版本 1872
JSON 政策文件 1873
進一步了解 1873
AWSCertificateManagerPrivateCAAuditor 1874
使用此政策 1874
政策詳細資訊 1874
政策版本 1874
JSON 政策文件 1874
進一步了解 1875
AWSCertificateManagerPrivateCAFullAccess 1875
使用此政策 1875
政策詳細資訊 1875
政策版本 1876
JSON 政策文件 1876
進一步了解 1876
AWSCertificateManagerPrivateCAPrivilegedUser 1876
使用此政策 1877
政策詳細資訊 1877
政策版本 1877
JSON 政策文件 1877
進一步了解 1878
AWSCertificateManagerPrivateCAReadOnly 1878
使用此政策 1879
政策詳細資訊 1879
政策版本 1879
JSON 政策文件 1879
進一步了解 1880
AWSCertificateManagerPrivateCAUser 1880
使用此政策 1880
政策詳細資訊 1880
政策版本 1880
JSON 政策文件 1880
進一步了解 1882

AWSCertificateManagerReadOnly 1882
使用此政策 1882
政策詳細資訊 1882
政策版本 1882
JSON 政策文件 1882
進一步了解 1883
AWSChatbotServiceLinkedRolePolicy 1883
使用此政策 1883
政策詳細資訊 1883
政策版本 1884
JSON 政策文件 1884
進一步了解 1884
AWSCleanRoomsFullAccess 1885
使用此政策 1885
政策詳細資訊 1885
政策版本 1885
JSON 政策文件 1885
進一步了解 1890
AWSCleanRoomsFullAccessNoQuerying 1890
使用此政策 1890
政策詳細資訊 1890
政策版本 1890
JSON 政策文件 1890
進一步了解 1895
AWSCleanRoomsMLFullAccess 1895
使用此政策 1895
政策詳細資訊 1896
政策版本 1896
JSON 政策文件 1896
進一步了解 1900
AWSCleanRoomsMLReadOnlyAccess 1900
使用此政策 1900
政策詳細資訊 1900
政策版本 1901
JSON 政策文件 1901
進一步了解 1902

AWSCleanRoomsReadOnlyAccess 1902
使用此政策 1902
政策詳細資訊 1902
政策版本 1903
JSON 政策文件 1903
進一步了解 1904
AWSCleanRoomsServiceRolePolicy 1904
使用此政策 1904
政策詳細資訊 1904
政策版本 1905
JSON 政策文件 1905
進一步了解 1905
AWSCloud9Administrator 1905
使用此政策 1906
政策詳細資訊 1906
政策版本 1906
JSON 政策文件 1906
進一步了解 1908
AWSCloud9EnvironmentMember 1908
使用此政策 1908
政策詳細資訊 1908
政策版本 1908
JSON 政策文件 1908
進一步了解 1910
AWSCloud9ServiceRolePolicy 1910
使用此政策 1910
政策詳細資訊 1910
政策版本 1911
JSON 政策文件 1911
進一步了解 1913
AWSCloud9SSMInstanceProfile 1913
使用此政策 1914
政策詳細資訊 1914
政策版本 1914
JSON 政策文件 1914
進一步了解 1914

AWSCloud9User 1915
使用此政策 1915
政策詳細資訊 1915
政策版本 1915
JSON 政策文件 1915
進一步了解 1918
AWSCloudFormationFullAccess 1918
使用此政策 1918
政策詳細資訊 1918
政策版本 1918
JSON 政策文件 1919
進一步了解 1919
AWSCloudFormationReadOnlyAccess 1919
使用此政策 1919
政策詳細資訊 1919
政策版本 1920
JSON 政策文件 1920
進一步了解 1920
AWSCloudFrontLogger 1921
使用此政策 1921
政策詳細資訊 1921
政策版本 1921
JSON 政策文件 1921
進一步了解 1922
AWSCloudFrontVPCOriginServiceRolePolicy 1922
使用此政策 1922
政策詳細資訊 1922
政策版本 1922
JSON 政策文件 1922
進一步了解 1925
AWSCloudHSMFullAccess 1925
使用此政策 1925
政策詳細資訊 1925
政策版本 1926
JSON 政策文件 1926
進一步了解 1926

AWSCloudHSMReadOnlyAccess 1926
使用此政策 1926
政策詳細資訊 1927
政策版本 1927
JSON 政策文件 1927
進一步了解 1927
AWSCloudHSMRole 1928
使用此政策 1928
政策詳細資訊 1928
政策版本 1928
JSON 政策文件 1928
進一步了解 1929
AWSCloudMapDiscoverInstanceAccess 1929
使用此政策 1929
政策詳細資訊 1929
政策版本 1929
JSON 政策文件 1930
進一步了解 1930
AWSCloudMapFullAccess 1930
使用此政策 1930
政策詳細資訊 1930
政策版本 1931
JSON 政策文件 1931
進一步了解 1932
AWSCloudMapReadOnlyAccess 1932
使用此政策 1932
政策詳細資訊 1932
政策版本 1932
JSON 政策文件 1932
進一步了解 1933
AWSCloudMapRegisterInstanceAccess 1933
使用此政策 1933
政策詳細資訊 1933
政策版本 1934
JSON 政策文件 1934
進一步了解 1934

AWSCloudShellFullAccess 1935
使用此政策 1935
政策詳細資訊 1935
政策版本 1935
JSON 政策文件 1935
進一步了解 1936
AWSCloudTrail_FullAccess 1936
使用此政策 1936
政策詳細資訊 1936
政策版本 1936
JSON 政策文件 1937
進一步了解 1939
AWSCloudTrail_ReadOnlyAccess 1939
使用此政策 1939
政策詳細資訊 1939
政策版本 1940
JSON 政策文件 1940
進一步了解 1940
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 1941
使用此政策 1941
政策詳細資訊 1941
政策版本 1941
JSON 政策文件 1941
進一步了解 1942
AWSCodeArtifactAdminAccess 1942
使用此政策 1942
政策詳細資訊 1942
政策版本 1942
JSON 政策文件 1942
進一步了解 1943
AWSCodeArtifactReadOnlyAccess 1943
使用此政策 1943
政策詳細資訊 1943
政策版本 1944
JSON 政策文件 1944
進一步了解 1944

AWSCodeBuildAdminAccess 1945
使用此政策 1945
政策詳細資訊 1945
政策版本 1945
JSON 政策文件 1945
進一步了解 1949
AWSCodeBuildDeveloperAccess 1949
使用此政策 1949
政策詳細資訊 1949
政策版本 1950
JSON 政策文件 1950
進一步了解 1952
AWSCodeBuildReadOnlyAccess 1953
使用此政策 1953
政策詳細資訊 1953
政策版本 1953
JSON 政策文件 1953
進一步了解 1955
AWSCodeCommitFullAccess 1955
使用此政策 1955
政策詳細資訊 1955
政策版本 1955
JSON 政策文件 1956
進一步了解 1960
AWSCodeCommitPowerUser 1960
使用此政策 1961
政策詳細資訊 1961
政策版本 1961
JSON 政策文件 1961
進一步了解 1966
AWSCodeCommitReadOnly 1966
使用此政策 1966
政策詳細資訊 1966
政策版本 1966
JSON 政策文件 1967
進一步了解 1969

AWSCodeDeployDeployerAccess 1969
使用此政策 1970
政策詳細資訊 1970
政策版本 1970
JSON 政策文件 1970
進一步了解 1972
AWSCodeDeployFullAccess 1972
使用此政策 1972
政策詳細資訊 1972
政策版本 1972
JSON 政策文件 1972
進一步了解 1974
AWSCodeDeployReadOnlyAccess 1974
使用此政策 1974
政策詳細資訊 1974
政策版本 1975
JSON 政策文件 1975
進一步了解 1976
AWSCodeDeployRole 1976
使用此政策 1976
政策詳細資訊 1976
政策版本 1976
JSON 政策文件 1977
進一步了解 1978
AWSCodeDeployRoleForCloudFormation 1978
使用此政策 1978
政策詳細資訊 1978
政策版本 1979
JSON 政策文件 1979
進一步了解 1979
AWSCodeDeployRoleForECS 1979
使用此政策 1980
政策詳細資訊 1980
政策版本 1980
JSON 政策文件 1980
進一步了解 1981

AWSCodeDeployRoleForECSLimited 1981
使用此政策 1981
政策詳細資訊 1981
政策版本 1982
JSON 政策文件 1982
進一步了解 1984
AWSCodeDeployRoleForLambda 1984
使用此政策 1984
政策詳細資訊 1984
政策版本 1984
JSON 政策文件 1984
進一步了解 1985
AWSCodeDeployRoleForLambdaLimited 1986
使用此政策 1986
政策詳細資訊 1986
政策版本 1986
JSON 政策文件 1986
進一步了解 1987
AWSCodePipeline_FullAccess 1988
使用此政策 1988
政策詳細資訊 1988
政策版本 1988
JSON 政策文件 1988
進一步了解 1992
AWSCodePipeline_ReadOnlyAccess 1992
使用此政策 1992
政策詳細資訊 1992
政策版本 1993
JSON 政策文件 1993
進一步了解 1994
AWSCodePipelineApproverAccess 1994
使用此政策 1994
政策詳細資訊 1994
政策版本 1995
JSON 政策文件 1995
進一步了解 1995

AWSCodePipelineCustomActionAccess 1995
使用此政策 1996
政策詳細資訊 1996
政策版本 1996
JSON 政策文件 1996
進一步了解 1996
AWSCodeStarFullAccess 1997
使用此政策 1997
政策詳細資訊 1997
政策版本 1997
JSON 政策文件 1997
進一步了解 1998
AWSCodeStarNotificationsServiceRolePolicy 1998
使用此政策 1998
政策詳細資訊 1999
政策版本 1999
JSON 政策文件 1999
進一步了解 2000
AWSCodeStarServiceRole 2000
使用此政策 2000
政策詳細資訊 2001
政策版本 2001
JSON 政策文件 2001
進一步了解 2006
AWSCompromisedKeyQuarantine 2006
使用此政策 2006
政策詳細資訊 2006
政策版本 2006
JSON 政策文件 2007
進一步了解 2008
AWSCompromisedKeyQuarantineV2 2008
使用此政策 2008
政策詳細資訊 2008
政策版本 2008
JSON 政策文件 2008
進一步了解 2011

AWSCompromisedKeyQuarantineV3 2011
使用此政策 2011
政策詳細資訊 2011
政策版本 2012
JSON 政策文件 2012
進一步了解 2015
AWSConfigMultiAccountSetupPolicy 2015
使用此政策 2015
政策詳細資訊 2015
政策版本 2015
JSON 政策文件 2016
進一步了解 2017
AWSConfigRemediationServiceRolePolicy 2018
使用此政策 2018
政策詳細資訊 2018
政策版本 2018
JSON 政策文件 2018
進一步了解 2019
AWSConfigRoleForOrganizations 2019
使用此政策 2019
政策詳細資訊 2019
政策版本 2019
JSON 政策文件 2020
進一步了解 2020
AWSConfigRulesExecutionRole 2020
使用此政策 2020
政策詳細資訊 2021
政策版本 2021
JSON 政策文件 2021
進一步了解 2022
AWSConfigServiceRolePolicy 2022
使用此政策 2022
政策詳細資訊 2022
政策版本 2022
JSON 政策文件 2022
進一步了解 2074

AWSConfigUserAccess 2074
使用此政策 2074
政策詳細資訊 2074
政策版本 2074
JSON 政策文件 2074
進一步了解 2075
AWSConnector 2075
使用此政策 2075
政策詳細資訊 2075
政策版本 2076
JSON 政策文件 2076
進一步了解 2078
AWSControlTowerAccountServiceRolePolicy 2078
使用此政策 2078
政策詳細資訊 2078
政策版本 2078
JSON 政策文件 2079
進一步了解 2084
AWSControlTowerCloudTrailRolePolicy 2084
使用此政策 2084
政策詳細資訊 2084
政策版本 2084
JSON 政策文件 2085
進一步了解 2085
AWSControlTowerIdentityCenterManagementPolicy 2085
使用此政策 2085
政策詳細資訊 2086
政策版本 2086
JSON 政策文件 2086
進一步了解 2087
AWSControlTowerServiceRolePolicy 2087
使用此政策 2087
政策詳細資訊 2088
政策版本 2088
JSON 政策文件 2088
進一步了解 2093

AWSCostAndUsageReportAutomationPolicy 2093
使用此政策 2093
政策詳細資訊 2093
政策版本 2094
JSON 政策文件 2094
進一步了解 2095
AWSDataExchangeDataGrantOwnerFullAccess 2095
使用此政策 2095
政策詳細資訊 2095
政策版本 2095
JSON 政策文件 2096
進一步了解 2097
AWSDataExchangeDataGrantReceiverFullAccess 2097
使用此政策 2097
政策詳細資訊 2097
政策版本 2098
JSON 政策文件 2098
進一步了解 2099
AWSDataExchangeFullAccess 2100
使用此政策 2100
政策詳細資訊 2100
政策版本 2100
JSON 政策文件 2100
進一步了解 2104
AWSDataExchangeProviderFullAccess 2104
使用此政策 2104
政策詳細資訊 2104
政策版本 2104
JSON 政策文件 2104
進一步了解 2108
AWSDataExchangeReadOnly 2109
使用此政策 2109
政策詳細資訊 2109
政策版本 2109
JSON 政策文件 2109
進一步了解 2110

AWSDataExchangeServiceRolePolicyForLicenseManagement 2111
使用此政策 2111
政策詳細資訊 2111
政策版本 2111
JSON 政策文件 2111
進一步了解 2112
AWSDataExchangeServiceRolePolicyForOrganizationDiscovery 2112
使用此政策 2112
政策詳細資訊 2112
政策版本 2112
JSON 政策文件 2113
進一步了解 2113
AWSDataExchangeSubscriberFullAccess 2113
使用此政策 2113
政策詳細資訊 2113
政策版本 2114
JSON 政策文件 2114
進一步了解 2116
AWSDataLifecycleManagerServiceRole 2116
使用此政策 2116
政策詳細資訊 2116
政策版本 2117
JSON 政策文件 2117
進一步了解 2118
AWSDataLifecycleManagerServiceRoleForAMIManagement 2118
使用此政策 2118
政策詳細資訊 2119
政策版本 2119
JSON 政策文件 2119
進一步了解 2120
AWSDataLifecycleManagerSSMFullAccess 2120
使用此政策 2121
政策詳細資訊 2121
政策版本 2121
JSON 政策文件 2121
進一步了解 2122

AWSDataPipeline_FullAccess 2123
使用此政策 2123
政策詳細資訊 2123
政策版本 2123
JSON 政策文件 2123
進一步了解 2124
AWSDataPipeline_PowerUser 2124
使用此政策 2125
政策詳細資訊 2125
政策版本 2125
JSON 政策文件 2125
進一步了解 2126
AWSDataSyncDiscoveryServiceRolePolicy 2126
使用此政策 2126
政策詳細資訊 2126
政策版本 2127
JSON 政策文件 2127
進一步了解 2128
AWSDataSyncFullAccess 2128
使用此政策 2128
政策詳細資訊 2128
政策版本 2128
JSON 政策文件 2129
進一步了解 2131
AWSDataSyncReadOnlyAccess 2131
使用此政策 2131
政策詳細資訊 2131
政策版本 2132
JSON 政策文件 2132
進一步了解 2132
AWSDataSyncServiceRolePolicy 2133
使用此政策 2133
政策詳細資訊 2133
政策版本 2133
JSON 政策文件 2133
進一步了解 2134

AWSDeadlineCloud-FleetWorker 2135
使用此政策 2135
政策詳細資訊 2135
政策版本 2135
JSON 政策文件 2135
進一步了解 2136
AWSDeadlineCloud-UserAccessFarms 2136
使用此政策 2136
政策詳細資訊 2136
政策版本 2136
JSON 政策文件 2137
進一步了解 2143
AWSDeadlineCloud-UserAccessFleets 2143
使用此政策 2143
政策詳細資訊 2143
政策版本 2143
JSON 政策文件 2144
進一步了解 2147
AWSDeadlineCloud-UserAccessJobs 2147
使用此政策 2148
政策詳細資訊 2148
政策版本 2148
JSON 政策文件 2148
進一步了解 2152
AWSDeadlineCloud-UserAccessQueues 2152
使用此政策 2152
政策詳細資訊 2152
政策版本 2153
JSON 政策文件 2153
進一步了解 2157
AWSDeadlineCloud-WorkerHost 2158
使用此政策 2158
政策詳細資訊 2158
政策版本 2158
JSON 政策文件 2158
進一步了解 2159

AWSDeepLensLambdaFunctionAccessPolicy 2160
使用此政策 2160
政策詳細資訊 2160
政策版本 2160
JSON 政策文件 2160
進一步了解 2161
AWSDeepLensServiceRolePolicy 2162
使用此政策 2162
政策詳細資訊 2162
政策版本 2162
JSON 政策文件 2162
進一步了解 2169
AWSDeepRacerAccountAdminAccess 2170
使用此政策 2170
政策詳細資訊 2170
政策版本 2170
JSON 政策文件 2170
進一步了解 2171
AWSDeepRacerCloudFormationAccessPolicy 2171
使用此政策 2171
政策詳細資訊 2171
政策版本 2171
JSON 政策文件 2172
進一步了解 2174
AWSDeepRacerDefaultMultiUserAccess 2175
使用此政策 2175
政策詳細資訊 2175
政策版本 2175
JSON 政策文件 2175
進一步了解 2177
AWSDeepRacerFullAccess 2177
使用此政策 2177
政策詳細資訊 2177
政策版本 2177
JSON 政策文件 2177
進一步了解 2178

AWSDeepRacerRoboMakerAccessPolicy 2179
使用此政策 2179
政策詳細資訊 2179
政策版本 2179
JSON 政策文件 2179
進一步了解 2181
AWSDeepRacerServiceRolePolicy 2181
使用此政策 2181
政策詳細資訊 2182
政策版本 2182
JSON 政策文件 2182
進一步了解 2185
AWSDenyAll 2185
使用此政策 2185
政策詳細資訊 2185
政策版本 2186
JSON 政策文件 2186
進一步了解 2186
AWSDeviceFarmFullAccess 2186
使用此政策 2187
政策詳細資訊 2187
政策版本 2187
JSON 政策文件 2187
進一步了解 2187
AWSDeviceFarmServiceRolePolicy 2188
使用此政策 2188
政策詳細資訊 2188
政策版本 2188
JSON 政策文件 2188
進一步了解 2190
AWSDeviceFarmTestGridServiceRolePolicy 2191
使用此政策 2191
政策詳細資訊 2191
政策版本 2191
JSON 政策文件 2191
進一步了解 2193

AWSDirectConnectFullAccess 2193
使用此政策 2194
政策詳細資訊 2194
政策版本 2194
JSON 政策文件 2194
進一步了解 2194
AWSDirectConnectReadOnlyAccess 2195
使用此政策 2195
政策詳細資訊 2195
政策版本 2195
JSON 政策文件 2195
進一步了解 2196
AWSDirectConnectServiceRolePolicy 2196
使用此政策 2196
政策詳細資訊 2196
政策版本 2196
JSON 政策文件 2197
進一步了解 2197
AWSDirectoryServiceDataFullAccess 2197
使用此政策 2197
政策詳細資訊 2197
政策版本 2198
JSON 政策文件 2198
進一步了解 2199
AWSDirectoryServiceDataReadOnlyAccess 2199
使用此政策 2199
政策詳細資訊 2199
政策版本 2199
JSON 政策文件 2199
進一步了解 2200
AWSDirectoryServiceFullAccess 2200
使用此政策 2200
政策詳細資訊 2201
政策版本 2201
JSON 政策文件 2201
進一步了解 2203

AWSDirectoryServiceReadOnlyAccess 2203
使用此政策 2203
政策詳細資訊 2203
政策版本 2203
JSON 政策文件 2204
進一步了解 2204
AWSDirectoryServiceServiceRolePolicy 2204
使用此政策 2205
政策詳細資訊 2205
政策版本 2205
JSON 政策文件 2205
進一步了解 2206
AWSDiscoveryContinuousExportFirehosePolicy 2206
使用此政策 2206
政策詳細資訊 2207
政策版本 2207
JSON 政策文件 2207
進一步了解 2208
AWSDMSFleetAdvisorServiceRolePolicy 2208
使用此政策 2208
政策詳細資訊 2208
政策版本 2209
JSON 政策文件 2209
進一步了解 2209
AWSDMSServerlessServiceRolePolicy 2209
使用此政策 2209
政策詳細資訊 2210
政策版本 2210
JSON 政策文件 2210
進一步了解 2213
AWSEC2CapacityManagerServiceRolePolicy 2213
使用此政策 2213
政策詳細資訊 2213
政策版本 2213
JSON 政策文件 2213
進一步了解 2214

AWSEC2CapacityReservationFleetRolePolicy 2214
使用此政策 2215
政策詳細資訊 2215
政策版本 2215
JSON 政策文件 2215
進一步了解 2216
AWSEC2FleetServiceRolePolicy 2216
使用此政策 2217
政策詳細資訊 2217
政策版本 2217
JSON 政策文件 2217
進一步了解 2219
AWSEC2SpotFleetServiceRolePolicy 2219
使用此政策 2219
政策詳細資訊 2220
政策版本 2220
JSON 政策文件 2220
進一步了解 2222
AWSEC2SpotServiceRolePolicy 2222
使用此政策 2222
政策詳細資訊 2222
政策版本 2222
JSON 政策文件 2223
進一步了解 2224
AWSEC2SqlHaInstancePolicy 2224
使用此政策 2224
政策詳細資訊 2224
政策版本 2225
JSON 政策文件 2225
進一步了解 2226
AWSEC2SqlHaServiceRolePolicy 2226
使用此政策 2226
政策詳細資訊 2227
政策版本 2227
JSON 政策文件 2227
進一步了解 2229

AWSEC2VssSnapshotPolicy 2229
使用此政策 2229
政策詳細資訊 2229
政策版本 2229
JSON 政策文件 2230
進一步了解 2233
AWSECRPullThroughCache_ServiceRolePolicy 2233
使用此政策 2233
政策詳細資訊 2233
政策版本 2233
JSON 政策文件 2234
進一步了解 2235
AWSElasticBeanstalkCustomPlatformforEC2Role 2235
使用此政策 2235
政策詳細資訊 2235
政策版本 2235
JSON 政策文件 2235
進一步了解 2237
AWSElasticBeanstalkEnhancedHealth 2237
使用此政策 2237
政策詳細資訊 2237
政策版本 2238
JSON 政策文件 2238
進一步了解 2239
AWSElasticBeanstalkMaintenance 2239
使用此政策 2239
政策詳細資訊 2239
政策版本 2240
JSON 政策文件 2240
進一步了解 2240
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 2241
使用此政策 2241
政策詳細資訊 2241
政策版本 2241
JSON 政策文件 2241
進一步了解 2248

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 2249
使用此政策 2249
政策詳細資訊 2249
政策版本 2249
JSON 政策文件 2249
進一步了解 2255
AWSElasticBeanstalkMulticontainerDocker 2255
使用此政策 2255
政策詳細資訊 2255
政策版本 2255
JSON 政策文件 2256
進一步了解 2257
AWSElasticBeanstalkReadOnly 2257
使用此政策 2258
政策詳細資訊 2258
政策版本 2258
JSON 政策文件 2258
進一步了解 2260
AWSElasticBeanstalkRoleCore 2260
使用此政策 2261
政策詳細資訊 2261
政策版本 2261
JSON 政策文件 2261
進一步了解 2266
AWSElasticBeanstalkRoleCWL 2266
使用此政策 2266
政策詳細資訊 2266
政策版本 2267
JSON 政策文件 2267
進一步了解 2267
AWSElasticBeanstalkRoleECS 2267
使用此政策 2268
政策詳細資訊 2268
政策版本 2268
JSON 政策文件 2268
進一步了解 2269

AWSElasticBeanstalkRoleRDS 2269
使用此政策 2269
政策詳細資訊 2269
政策版本 2270
JSON 政策文件 2270
進一步了解 2270
AWSElasticBeanstalkRoleSNS 2271
使用此政策 2271
政策詳細資訊 2271
政策版本 2271
JSON 政策文件 2271
進一步了解 2272
AWSElasticBeanstalkRoleWorkerTier 2272
使用此政策 2272
政策詳細資訊 2272
政策版本 2273
JSON 政策文件 2273
進一步了解 2274
AWSElasticBeanstalkService 2274
使用此政策 2274
政策詳細資訊 2274
政策版本 2274
JSON 政策文件 2274
進一步了解 2279
AWSElasticBeanstalkServiceRolePolicy 2279
使用此政策 2279
政策詳細資訊 2279
政策版本 2279
JSON 政策文件 2280
進一步了解 2281
AWSElasticBeanstalkWebTier 2281
使用此政策 2281
政策詳細資訊 2281
政策版本 2282
JSON 政策文件 2282
進一步了解 2284

AWSElasticBeanstalkWorkerTier 2284
使用此政策 2284
政策詳細資訊 2284
政策版本 2284
JSON 政策文件 2285
進一步了解 2287
AWSElasticDisasterRecoveryAgentInstallationPolicy 2288
使用此政策 2288
政策詳細資訊 2288
政策版本 2288
JSON 政策文件 2288
進一步了解 2290
AWSElasticDisasterRecoveryAgentPolicy 2290
使用此政策 2290
政策詳細資訊 2290
政策版本 2290
JSON 政策文件 2291
進一步了解 2291
AWSElasticDisasterRecoveryConsoleFullAccess 2292
使用此政策 2292
政策詳細資訊 2292
政策版本 2292
JSON 政策文件 2292
進一步了解 2302
AWSElasticDisasterRecoveryConsoleFullAccess_v2 2303
使用此政策 2303
政策詳細資訊 2303
政策版本 2303
JSON 政策文件 2303
進一步了解 2319
AWSElasticDisasterRecoveryConversionServerPolicy 2319
使用此政策 2319
政策詳細資訊 2319
政策版本 2319
JSON 政策文件 2320
進一步了解 2320

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 2320
使用此政策 2321
政策詳細資訊 2321
政策版本 2321
JSON 政策文件 2321
進一步了解 2322
AWSElasticDisasterRecoveryEc2InstancePolicy 2322
使用此政策 2322
政策詳細資訊 2322
政策版本 2323
JSON 政策文件 2323
進一步了解 2325
AWSElasticDisasterRecoveryFailbackInstallationPolicy 2325
使用此政策 2325
政策詳細資訊 2325
政策版本 2326
JSON 政策文件 2326
進一步了解 2326
AWSElasticDisasterRecoveryFailbackPolicy 2327
使用此政策 2327
政策詳細資訊 2327
政策版本 2327
JSON 政策文件 2327
進一步了解 2329
AWSElasticDisasterRecoveryLaunchActionsPolicy 2329
使用此政策 2329
政策詳細資訊 2329
政策版本 2329
JSON 政策文件 2329
進一步了解 2335
AWSElasticDisasterRecoveryNetworkReplicationPolicy 2336
使用此政策 2336
政策詳細資訊 2336
政策版本 2336
JSON 政策文件 2336
進一步了解 2337

AWSElasticDisasterRecoveryReadOnlyAccess 2337
使用此政策 2337
政策詳細資訊 2337
政策版本 2338
JSON 政策文件 2338
進一步了解 2340
AWSElasticDisasterRecoveryRecoveryInstancePolicy 2340
使用此政策 2340
政策詳細資訊 2341
政策版本 2341
JSON 政策文件 2341
進一步了解 2343
AWSElasticDisasterRecoveryReplicationServerPolicy 2344
使用此政策 2344
政策詳細資訊 2344
政策版本 2344
JSON 政策文件 2344
進一步了解 2347
AWSElasticDisasterRecoveryServiceRolePolicy 2347
使用此政策 2347
政策詳細資訊 2347
政策版本 2347
JSON 政策文件 2347
進一步了解 2357
AWSElasticDisasterRecoveryStagingAccountPolicy 2358
使用此政策 2358
政策詳細資訊 2358
政策版本 2358
JSON 政策文件 2358
進一步了解 2359
AWSElasticDisasterRecoveryStagingAccountPolicy_v2 2359
使用此政策 2360
政策詳細資訊 2360
政策版本 2360
JSON 政策文件 2360
進一步了解 2361

AWSElasticLoadBalancingClassicServiceRolePolicy 2361
使用此政策 2362
政策詳細資訊 2362
政策版本 2362
JSON 政策文件 2362
進一步了解 2363
AWSElasticLoadBalancingServiceRolePolicy 2363
使用此政策 2363
政策詳細資訊 2363
政策版本 2364
JSON 政策文件 2364
進一步了解 2365
AWSElementalMediaConnectCreateBridge 2365
使用此政策 2365
政策詳細資訊 2365
政策版本 2365
JSON 政策文件 2366
進一步了解 2366
AWSElementalMediaConnectCreateFlow 2366
使用此政策 2366
政策詳細資訊 2367
政策版本 2367
JSON 政策文件 2367
進一步了解 2368
AWSElementalMediaConnectDeleteBridge 2368
使用此政策 2368
政策詳細資訊 2368
政策版本 2368
JSON 政策文件 2369
進一步了解 2369
AWSElementalMediaConnectDeleteFlow 2369
使用此政策 2369
政策詳細資訊 2370
政策版本 2370
JSON 政策文件 2370
進一步了解 2371

AWSElementalMediaConnectFullAccess 2371
使用此政策 2371
政策詳細資訊 2371
政策版本 2371
JSON 政策文件 2371
進一步了解 2372
AWSElementalMediaConnectReadOnlyAccess 2372
使用此政策 2372
政策詳細資訊 2372
政策版本 2372
JSON 政策文件 2373
進一步了解 2373
AWSElementalMediaConvertFullAccess 2373
使用此政策 2374
政策詳細資訊 2374
政策版本 2374
JSON 政策文件 2374
進一步了解 2375
AWSElementalMediaConvertReadOnly 2375
使用此政策 2375
政策詳細資訊 2375
政策版本 2375
JSON 政策文件 2376
進一步了解 2376
AWSElementalMediaLiveFullAccess 2376
使用此政策 2376
政策詳細資訊 2377
政策版本 2377
JSON 政策文件 2377
進一步了解 2377
AWSElementalMediaLiveReadOnly 2377
使用此政策 2378
政策詳細資訊 2378
政策版本 2378
JSON 政策文件 2378
進一步了解 2378

AWSElementalMediaPackageFullAccess 2379
使用此政策 2379
政策詳細資訊 2379
政策版本 2379
JSON 政策文件 2379
進一步了解 2380
AWSElementalMediaPackageReadOnly 2380
使用此政策 2380
政策詳細資訊 2380
政策版本 2380
JSON 政策文件 2380
進一步了解 2381
AWSElementalMediaPackageV2FullAccess 2381
使用此政策 2381
政策詳細資訊 2381
政策版本 2381
JSON 政策文件 2382
進一步了解 2382
AWSElementalMediaPackageV2ReadOnly 2382
使用此政策 2382
政策詳細資訊 2382
政策版本 2383
JSON 政策文件 2383
進一步了解 2383
AWSElementalMediaStoreFullAccess 2383
使用此政策 2383
政策詳細資訊 2384
政策版本 2384
JSON 政策文件 2384
進一步了解 2384
AWSElementalMediaStoreReadOnly 2385
使用此政策 2385
政策詳細資訊 2385
政策版本 2385
JSON 政策文件 2385
進一步了解 2386

AWSElementalMediaTailorFullAccess 2386
使用此政策 2386
政策詳細資訊 2386
政策版本 2386
JSON 政策文件 2387
進一步了解 2387
AWSElementalMediaTailorReadOnly 2387
使用此政策 2387
政策詳細資訊 2387
政策版本 2388
JSON 政策文件 2388
進一步了解 2388
AWSEnhancedClassicNetworkingMangementPolicy 2388
使用此政策 2388
政策詳細資訊 2389
政策版本 2389
JSON 政策文件 2389
進一步了解 2389
AWSEntityResolutionConsoleFullAccess 2390
使用此政策 2390
政策詳細資訊 2390
政策版本 2390
JSON 政策文件 2390
進一步了解 2393
AWSEntityResolutionConsoleReadOnlyAccess 2394
使用此政策 2394
政策詳細資訊 2394
政策版本 2394
JSON 政策文件 2394
進一步了解 2395
AWSFaultInjectionSimulatorEC2Access 2395
使用此政策 2395
政策詳細資訊 2395
政策版本 2395
JSON 政策文件 2396
進一步了解 2397

AWSFaultInjectionSimulatorECSAccess 2397
使用此政策 2398
政策詳細資訊 2398
政策版本 2398
JSON 政策文件 2398
進一步了解 2400
AWSFaultInjectionSimulatorEKSAccess 2400
使用此政策 2401
政策詳細資訊 2401
政策版本 2401
JSON 政策文件 2401
進一步了解 2402
AWSFaultInjectionSimulatorNetworkAccess 2402
使用此政策 2403
政策詳細資訊 2403
政策版本 2403
JSON 政策文件 2403
進一步了解 2410
AWSFaultInjectionSimulatorRDSAccess 2410
使用此政策 2410
政策詳細資訊 2410
政策版本 2411
JSON 政策文件 2411
進一步了解 2412
AWSFaultInjectionSimulatorSSMAccess 2412
使用此政策 2412
政策詳細資訊 2412
政策版本 2413
JSON 政策文件 2413
進一步了解 2414
AWSFinSpaceServiceRolePolicy 2414
使用此政策 2414
政策詳細資訊 2414
政策版本 2415
JSON 政策文件 2415
進一步了解 2415

AWSFMAdminFullAccess 2416
使用此政策 2416
政策詳細資訊 2416
政策版本 2416
JSON 政策文件 2416
進一步了解 2418
AWSFMAdminReadOnlyAccess 2418
使用此政策 2418
政策詳細資訊 2418
政策版本 2419
JSON 政策文件 2419
進一步了解 2420
AWSFMMemberReadOnlyAccess 2420
使用此政策 2421
政策詳細資訊 2421
政策版本 2421
JSON 政策文件 2421
進一步了解 2422
AWSForWordPressPluginPolicy 2422
使用此政策 2422
政策詳細資訊 2422
政策版本 2422
JSON 政策文件 2422
進一步了解 2424
AWSGitSyncServiceRolePolicy 2424
使用此政策 2425
政策詳細資訊 2425
政策版本 2425
JSON 政策文件 2425
進一步了解 2426
AWSGlobalAcceleratorSLRPolicy 2426
使用此政策 2426
政策詳細資訊 2426
政策版本 2426
JSON 政策文件 2426
進一步了解 2428

AWSGlueConsoleFullAccess 2428
使用此政策 2428
政策詳細資訊 2428
政策版本 2429
JSON 政策文件 2429
進一步了解 2433
AWSGlueConsoleSageMakerNotebookFullAccess 2433
使用此政策 2433
政策詳細資訊 2433
政策版本 2434
JSON 政策文件 2434
進一步了解 2439
AwsGlueDataBrewFullAccessPolicy 2439
使用此政策 2439
政策詳細資訊 2439
政策版本 2440
JSON 政策文件 2440
進一步了解 2445
AWSGlueDataBrewServiceRole 2445
使用此政策 2445
政策詳細資訊 2445
政策版本 2445
JSON 政策文件 2446
進一步了解 2448
AWSGlueSchemaRegistryFullAccess 2449
使用此政策 2449
政策詳細資訊 2449
政策版本 2449
JSON 政策文件 2449
進一步了解 2450
AWSGlueSchemaRegistryReadonlyAccess 2451
使用此政策 2451
政策詳細資訊 2451
政策版本 2451
JSON 政策文件 2451
進一步了解 2452

AWSGlueServiceNotebookRole 2452
使用此政策 2452
政策詳細資訊 2452
政策版本 2453
JSON 政策文件 2453
進一步了解 2455
AWSGlueServiceRole 2455
使用此政策 2455
政策詳細資訊 2455
政策版本 2456
JSON 政策文件 2456
進一步了解 2458
AwsGlueSessionUserRestrictedNotebookPolicy 2458
使用此政策 2458
政策詳細資訊 2458
政策版本 2459
JSON 政策文件 2459
進一步了解 2462
AwsGlueSessionUserRestrictedNotebookServiceRole 2462
使用此政策 2462
政策詳細資訊 2462
政策版本 2462
JSON 政策文件 2463
進一步了解 2466
AwsGlueSessionUserRestrictedPolicy 2467
使用此政策 2467
政策詳細資訊 2467
政策版本 2467
JSON 政策文件 2467
進一步了解 2470
AwsGlueSessionUserRestrictedServiceRole 2470
使用此政策 2470
政策詳細資訊 2471
政策版本 2471
JSON 政策文件 2471
進一步了解 2475

AWSGrafanaAccountAdministrator 2476
使用此政策 2476
政策詳細資訊 2476
政策版本 2476
JSON 政策文件 2476
進一步了解 2477
AWSGrafanaConsoleReadOnlyAccess 2477
使用此政策 2477
政策詳細資訊 2478
政策版本 2478
JSON 政策文件 2478
進一步了解 2478
AWSGrafanaWorkspacePermissionManagement 2479
使用此政策 2479
政策詳細資訊 2479
政策版本 2479
JSON 政策文件 2479
進一步了解 2480
AWSGrafanaWorkspacePermissionManagementV2 2480
使用此政策 2480
政策詳細資訊 2481
政策版本 2481
JSON 政策文件 2481
進一步了解 2482
AWSGreengrassFullAccess 2482
使用此政策 2482
政策詳細資訊 2482
政策版本 2482
JSON 政策文件 2483
進一步了解 2483
AWSGreengrassReadOnlyAccess 2483
使用此政策 2483
政策詳細資訊 2483
政策版本 2484
JSON 政策文件 2484
進一步了解 2484

AWSGreengrassResourceAccessRolePolicy 2484
使用此政策 2485
政策詳細資訊 2485
政策版本 2485
JSON 政策文件 2485
進一步了解 2487
AWSGroundStationAgentInstancePolicy 2488
使用此政策 2488
政策詳細資訊 2488
政策版本 2488
JSON 政策文件 2488
進一步了解 2489
AWSHealth_EventProcessorServiceRolePolicy 2489
使用此政策 2489
政策詳細資訊 2489
政策版本 2489
JSON 政策文件 2490
進一步了解 2490
AWSHealthFullAccess 2490
使用此政策 2491
政策詳細資訊 2491
政策版本 2491
JSON 政策文件 2491
進一步了解 2492
AWSHealthImagingFullAccess 2492
使用此政策 2492
政策詳細資訊 2492
政策版本 2493
JSON 政策文件 2493
進一步了解 2493
AWSHealthImagingReadOnlyAccess 2494
使用此政策 2494
政策詳細資訊 2494
政策版本 2494
JSON 政策文件 2494
進一步了解 2495

AWSHealthImagingServiceRolePolicy 2495
使用此政策 2495
政策詳細資訊 2495
政策版本 2496
JSON 政策文件 2496
進一步了解 2496
AWSHealthOmicsServiceLinkedRolePolicy 2496
使用此政策 2497
政策詳細資訊 2497
政策版本 2497
JSON 政策文件 2497
進一步了解 2499
AWSIAMIdentityCenterAllowListForIdentityContext 2499
使用此政策 2499
政策詳細資訊 2500
政策版本 2500
JSON 政策文件 2500
進一步了解 2503
AWSIdentityCenterExternalManagementPolicy 2503
使用此政策 2503
政策詳細資訊 2504
政策版本 2504
JSON 政策文件 2504
進一步了解 2506
AWSIdentitySyncFullAccess 2506
使用此政策 2506
政策詳細資訊 2506
政策版本 2506
JSON 政策文件 2506
進一步了解 2507
AWSIdentitySyncReadOnlyAccess 2507
使用此政策 2508
政策詳細資訊 2508
政策版本 2508
JSON 政策文件 2508
進一步了解 2508

AWSImageBuilderFullAccess 2509
使用此政策 2509
政策詳細資訊 2509
政策版本 2509
JSON 政策文件 2509
進一步了解 2512
AWSImageBuilderReadOnlyAccess 2512
使用此政策 2512
政策詳細資訊 2512
政策版本 2513
JSON 政策文件 2513
進一步了解 2513
AWSImportExportFullAccess 2514
使用此政策 2514
政策詳細資訊 2514
政策版本 2514
JSON 政策文件 2514
進一步了解 2515
AWSImportExportReadOnlyAccess 2515
使用此政策 2515
政策詳細資訊 2515
政策版本 2515
JSON 政策文件 2515
進一步了解 2516
AWSIncidentManagerIncidentAccessServiceRolePolicy 2516
使用此政策 2516
政策詳細資訊 2516
政策版本 2517
JSON 政策文件 2517
進一步了解 2517
AWSIncidentManagerResolverAccess 2517
使用此政策 2518
政策詳細資訊 2518
政策版本 2518
JSON 政策文件 2518
進一步了解 2519

AWSIncidentManagerServiceRolePolicy 2519
使用此政策 2519
政策詳細資訊 2520
政策版本 2520
JSON 政策文件 2520
進一步了解 2521
AWSIoT1ClickFullAccess 2521
使用此政策 2521
政策詳細資訊 2521
政策版本 2522
JSON 政策文件 2522
進一步了解 2522
AWSIoT1ClickReadOnlyAccess 2522
使用此政策 2523
政策詳細資訊 2523
政策版本 2523
JSON 政策文件 2523
進一步了解 2523
AWSIoTAnalyticsFullAccess 2524
使用此政策 2524
政策詳細資訊 2524
政策版本 2524
JSON 政策文件 2524
進一步了解 2525
AWSIoTAnalyticsReadOnlyAccess 2525
使用此政策 2525
政策詳細資訊 2525
政策版本 2525
JSON 政策文件 2525
進一步了解 2526
AWSIoTConfigAccess 2526
使用此政策 2526
政策詳細資訊 2526
政策版本 2527
JSON 政策文件 2527
進一步了解 2531

AWSIoTConfigReadOnlyAccess 2531
使用此政策 2531
政策詳細資訊 2531
政策版本 2531
JSON 政策文件 2531
進一步了解 2533
AWSIoTDataAccess 2534
使用此政策 2534
政策詳細資訊 2534
政策版本 2534
JSON 政策文件 2534
進一步了解 2535
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 2535
使用此政策 2535
政策詳細資訊 2535
政策版本 2535
JSON 政策文件 2536
進一步了解 2536
AWSIoTDeviceDefenderAudit 2536
使用此政策 2536
政策詳細資訊 2537
政策版本 2537
JSON 政策文件 2537
進一步了解 2538
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 2538
使用此政策 2538
政策詳細資訊 2538
政策版本 2538
JSON 政策文件 2539
進一步了解 2539
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 2540
使用此政策 2540
政策詳細資訊 2540
政策版本 2540
JSON 政策文件 2540
進一步了解 2541

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 2541
使用此政策 2541
政策詳細資訊 2541
政策版本 2541
JSON 政策文件 2542
進一步了解 2542
AWSIoTDeviceDefenderUpdateCACertMitigationAction 2542
使用此政策 2542
政策詳細資訊 2542
政策版本 2543
JSON 政策文件 2543
進一步了解 2543
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 2543
使用此政策 2544
政策詳細資訊 2544
政策版本 2544
JSON 政策文件 2544
進一步了解 2545
AWSIoTDeviceTesterForFreeRTOSFullAccess 2545
使用此政策 2545
政策詳細資訊 2545
政策版本 2545
JSON 政策文件 2545
進一步了解 2551
AWSIoTDeviceTesterForGreengrassFullAccess 2552
使用此政策 2552
政策詳細資訊 2552
政策版本 2552
JSON 政策文件 2552
進一步了解 2555
AWSIoTEventsFullAccess 2555
使用此政策 2556
政策詳細資訊 2556
政策版本 2556
JSON 政策文件 2556
進一步了解 2556

AWSIoTEventsReadOnlyAccess 2557
使用此政策 2557
政策詳細資訊 2557
政策版本 2557
JSON 政策文件 2557
進一步了解 2558
AWSIoTFleetHubFederationAccess 2558
使用此政策 2558
政策詳細資訊 2558
政策版本 2558
JSON 政策文件 2559
進一步了解 2560
AWSIoTFleetwiseServiceRolePolicy 2560
使用此政策 2561
政策詳細資訊 2561
政策版本 2561
JSON 政策文件 2561
進一步了解 2562
AWSIoTFullAccess 2562
使用此政策 2562
政策詳細資訊 2562
政策版本 2562
JSON 政策文件 2562
進一步了解 2563
AWSIoTLogging 2563
使用此政策 2563
政策詳細資訊 2563
政策版本 2564
JSON 政策文件 2564
進一步了解 2564
AWSIoTManagedIntegrationsFullAccess 2564
使用此政策 2565
政策詳細資訊 2565
政策版本 2565
JSON 政策文件 2565
進一步了解 2566

AWSIoTManagedIntegrationsRolePolicy 2566
使用此政策 2566
政策詳細資訊 2566
政策版本 2566
JSON 政策文件 2567
進一步了解 2568
AWSIoTOTAUpdate 2568
使用此政策 2568
政策詳細資訊 2568
政策版本 2568
JSON 政策文件 2569
進一步了解 2569
AWSIotRoboRunnerFullAccess 2569
使用此政策 2569
政策詳細資訊 2569
政策版本 2570
JSON 政策文件 2570
進一步了解 2570
AWSIotRoboRunnerReadOnly 2571
使用此政策 2571
政策詳細資訊 2571
政策版本 2571
JSON 政策文件 2571
進一步了解 2572
AWSIotRoboRunnerServiceRolePolicy 2572
使用此政策 2572
政策詳細資訊 2572
政策版本 2572
JSON 政策文件 2573
進一步了解 2573
AWSIoTRuleActions 2573
使用此政策 2573
政策詳細資訊 2573
政策版本 2574
JSON 政策文件 2574
進一步了解 2574

AWSIoTSiteWiseConsoleFullAccess 2575
使用此政策 2575
政策詳細資訊 2575
政策版本 2575
JSON 政策文件 2575
進一步了解 2577
AWSIoTSiteWiseFullAccess 2577
使用此政策 2578
政策詳細資訊 2578
政策版本 2578
JSON 政策文件 2578
進一步了解 2578
AWSIoTSiteWiseMonitorPortalAccess 2579
使用此政策 2579
政策詳細資訊 2579
政策版本 2579
JSON 政策文件 2579
進一步了解 2580
AWSIoTSiteWiseMonitorServiceRolePolicy 2581
使用此政策 2581
政策詳細資訊 2581
政策版本 2581
JSON 政策文件 2581
進一步了解 2582
AWSIoTSiteWiseReadOnlyAccess 2582
使用此政策 2582
政策詳細資訊 2583
政策版本 2583
JSON 政策文件 2583
進一步了解 2585
AWSIoTThingsRegistration 2585
使用此政策 2585
政策詳細資訊 2585
政策版本 2585
JSON 政策文件 2585
進一步了解 2586

AWSIoTTwinMakerServiceRolePolicy 2587
使用此政策 2587
政策詳細資訊 2587
政策版本 2587
JSON 政策文件 2587
進一步了解 2589
AWSIoTWirelessDataAccess 2589
使用此政策 2589
政策詳細資訊 2589
政策版本 2589
JSON 政策文件 2590
進一步了解 2590
AWSIoTWirelessFullAccess 2590
使用此政策 2590
政策詳細資訊 2590
政策版本 2591
JSON 政策文件 2591
進一步了解 2591
AWSIoTWirelessFullPublishAccess 2591
使用此政策 2591
政策詳細資訊 2592
政策版本 2592
JSON 政策文件 2592
進一步了解 2592
AWSIoTWirelessGatewayCertManager 2593
使用此政策 2593
政策詳細資訊 2593
政策版本 2593
JSON 政策文件 2593
進一步了解 2594
AWSIoTWirelessLogging 2594
使用此政策 2594
政策詳細資訊 2594
政策版本 2594
JSON 政策文件 2594
進一步了解 2595

AWSIoTWirelessReadOnlyAccess 2595
使用此政策 2595
政策詳細資訊 2595
政策版本 2596
JSON 政策文件 2596
進一步了解 2596
AWSIPAMServiceRolePolicy 2596
使用此政策 2596
政策詳細資訊 2597
政策版本 2597
JSON 政策文件 2597
進一步了解 2599
AWSIQContractServiceRolePolicy 2599
使用此政策 2599
政策詳細資訊 2599
政策版本 2599
JSON 政策文件 2600
進一步了解 2600
AWSIQFullAccess 2600
使用此政策 2600
政策詳細資訊 2600
政策版本 2601
JSON 政策文件 2601
進一步了解 2601
AWSIQPermissionServiceRolePolicy 2602
使用此政策 2602
政策詳細資訊 2602
政策版本 2602
JSON 政策文件 2602
進一步了解 2603
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2603
使用此政策 2603
政策詳細資訊 2604
政策版本 2604
JSON 政策文件 2604
進一步了解 2605

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2605
使用此政策 2605
政策詳細資訊 2605
政策版本 2605
JSON 政策文件 2605
進一步了解 2606
AWSKeyManagementServicePowerUser 2606
使用此政策 2606
政策詳細資訊 2606
政策版本 2606
JSON 政策文件 2607
進一步了解 2607
AWSLakeFormationCrossAccountManager 2607
使用此政策 2608
政策詳細資訊 2608
政策版本 2608
JSON 政策文件 2608
進一步了解 2610
AWSLakeFormationDataAdmin 2610
使用此政策 2610
政策詳細資訊 2610
政策版本 2611
JSON 政策文件 2611
進一步了解 2612
AWSLambda_FullAccess 2612
使用此政策 2612
政策詳細資訊 2613
政策版本 2613
JSON 政策文件 2613
進一步了解 2615
AWSLambda_ReadOnlyAccess 2615
使用此政策 2615
政策詳細資訊 2615
政策版本 2615
JSON 政策文件 2615
進一步了解 2617

AWSLambdaBasicDurableExecutionRolePolicy 2617
使用此政策 2617
政策詳細資訊 2617
政策版本 2617
JSON 政策文件 2618
進一步了解 2618
AWSLambdaBasicExecutionRole 2618
使用此政策 2618
政策詳細資訊 2618
政策版本 2619
JSON 政策文件 2619
進一步了解 2619
AWSLambdaDynamoDBExecutionRole 2619
使用此政策 2620
政策詳細資訊 2620
政策版本 2620
JSON 政策文件 2620
進一步了解 2621
AWSLambdaENIManagementAccess 2621
使用此政策 2621
政策詳細資訊 2621
政策版本 2621
JSON 政策文件 2621
進一步了解 2622
AWSLambdaExecute 2622
使用此政策 2622
政策詳細資訊 2622
政策版本 2623
JSON 政策文件 2623
進一步了解 2623
AWSLambdaFullAccess 2624
使用此政策 2624
政策詳細資訊 2624
政策版本 2624
JSON 政策文件 2624
進一步了解 2626

AWSLambdaInvocation-DynamoDB 2626
使用此政策 2626
政策詳細資訊 2626
政策版本 2626
JSON 政策文件 2627
進一步了解 2627
AWSLambdaKinesisExecutionRole 2627
使用此政策 2628
政策詳細資訊 2628
政策版本 2628
JSON 政策文件 2628
進一步了解 2629
AWSLambdaManagedEC2ResourceOperator 2629
使用此政策 2629
政策詳細資訊 2629
政策版本 2629
JSON 政策文件 2629
進一步了解 2631
AWSLambdaMSKExecutionRole 2631
使用此政策 2631
政策詳細資訊 2631
政策版本 2632
JSON 政策文件 2632
進一步了解 2632
AWSLambdaReplicator 2633
使用此政策 2633
政策詳細資訊 2633
政策版本 2633
JSON 政策文件 2633
進一步了解 2634
AWSLambdaRole 2634
使用此政策 2635
政策詳細資訊 2635
政策版本 2635
JSON 政策文件 2635
進一步了解 2635

AWSLambdaServiceRolePolicy 2636
使用此政策 2636
政策詳細資訊 2636
政策版本 2636
JSON 政策文件 2636
進一步了解 2637
AWSLambdaSQSQueueExecutionRole 2637
使用此政策 2637
政策詳細資訊 2637
政策版本 2638
JSON 政策文件 2638
進一步了解 2638
AWSLambdaVPCAccessExecutionRole 2639
使用此政策 2639
政策詳細資訊 2639
政策版本 2639
JSON 政策文件 2639
進一步了解 2640
AWSLicenseManagerConsumptionPolicy 2640
使用此政策 2640
政策詳細資訊 2640
政策版本 2640
JSON 政策文件 2641
進一步了解 2641
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 2641
使用此政策 2641
政策詳細資訊 2641
政策版本 2642
JSON 政策文件 2642
進一步了解 2644
AWSLicenseManagerMasterAccountRolePolicy 2644
使用此政策 2644
政策詳細資訊 2644
政策版本 2644
JSON 政策文件 2644
進一步了解 2649

AWSLicenseManagerMemberAccountRolePolicy 2649
使用此政策 2650
政策詳細資訊 2650
政策版本 2650
JSON 政策文件 2650
進一步了解 2651
AWSLicenseManagerServiceRolePolicy 2651
使用此政策 2651
政策詳細資訊 2652
政策版本 2652
JSON 政策文件 2652
進一步了解 2655
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 2656
使用此政策 2656
政策詳細資訊 2656
政策版本 2656
JSON 政策文件 2656
進一步了解 2659
AWSM2ServicePolicy 2659
使用此政策 2660
政策詳細資訊 2660
政策版本 2660
JSON 政策文件 2660
進一步了解 2661
AWSManagedServices_ContactsServiceRolePolicy 2662
使用此政策 2662
政策詳細資訊 2662
政策版本 2662
JSON 政策文件 2662
進一步了解 2663
AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 2663
使用此政策 2663
政策詳細資訊 2663
政策版本 2664
JSON 政策文件 2664
進一步了解 2665

AWSManagedServices_EventsServiceRolePolicy 2665
使用此政策 2666
政策詳細資訊 2666
政策版本 2666
JSON 政策文件 2666
進一步了解 2667
AWSManagedServices_SelfServiceReporting_ServiceRolePolicy 2667
使用此政策 2667
政策詳細資訊 2667
政策版本 2667
JSON 政策文件 2668
進一步了解 2668
AWSManagedServicesDeploymentToolkitPolicy 2668
使用此政策 2668
政策詳細資訊 2669
政策版本 2669
JSON 政策文件 2669
進一步了解 2671
AWSManagementConsoleAdministratorAccess 2671
使用此政策 2671
政策詳細資訊 2671
政策版本 2672
JSON 政策文件 2672
進一步了解 2674
AWSManagementConsoleBasicUserAccess 2674
使用此政策 2674
政策詳細資訊 2674
政策版本 2675
JSON 政策文件 2675
進一步了解 2676
AWSMarketplaceAmiIngestion 2676
使用此政策 2676
政策詳細資訊 2676
政策版本 2677
JSON 政策文件 2677
進一步了解 2677

AWSMarketplaceDeploymentServiceRolePolicy 2678
使用此政策 2678
政策詳細資訊 2678
政策版本 2678
JSON 政策文件 2678
進一步了解 2680
AWSMarketplaceFullAccess 2680
使用此政策 2680
政策詳細資訊 2680
政策版本 2680
JSON 政策文件 2680
進一步了解 2682
AWSMarketplaceGetEntitlements 2682
使用此政策 2682
政策詳細資訊 2683
政策版本 2683
JSON 政策文件 2683
進一步了解 2683
AWSMarketplaceImageBuildFullAccess 2684
使用此政策 2684
政策詳細資訊 2684
政策版本 2684
JSON 政策文件 2684
進一步了解 2688
AWSMarketplaceLicenseManagementServiceRolePolicy 2688
使用此政策 2688
政策詳細資訊 2688
政策版本 2688
JSON 政策文件 2689
進一步了解 2689
AWSMarketplaceManageSubscriptions 2689
使用此政策 2689
政策詳細資訊 2690
政策版本 2690
JSON 政策文件 2690
進一步了解 2692

AWSMarketplaceMeteringFullAccess 2692
使用此政策 2692
政策詳細資訊 2693
政策版本 2693
JSON 政策文件 2693
進一步了解 2693
AWSMarketplaceMeteringRegisterUsage 2694
使用此政策 2694
政策詳細資訊 2694
政策版本 2694
JSON 政策文件 2694
進一步了解 2695
AWSMarketplaceProcurementSystemAdminFullAccess 2695
使用此政策 2695
政策詳細資訊 2695
政策版本 2695
JSON 政策文件 2695
進一步了解 2696
AWSMarketplacePurchaseOrdersServiceRolePolicy 2696
使用此政策 2696
政策詳細資訊 2696
政策版本 2697
JSON 政策文件 2697
進一步了解 2697
AWSMarketplaceRead-only 2697
使用此政策 2698
政策詳細資訊 2698
政策版本 2698
JSON 政策文件 2698
進一步了解 2699
AWSMarketplaceResaleAuthorizationServiceRolePolicy 2699
使用此政策 2700
政策詳細資訊 2700
政策版本 2700
JSON 政策文件 2700
進一步了解 2702

AWSMarketplaceSellerFullAccess 2703
使用此政策 2703
政策詳細資訊 2703
政策版本 2703
JSON 政策文件 2703
進一步了解 2708
AWSMarketplaceSellerOfferManagement 2708
使用此政策 2708
政策詳細資訊 2708
政策版本 2708
JSON 政策文件 2708
進一步了解 2710
AWSMarketplaceSellerProductsFullAccess 2711
使用此政策 2711
政策詳細資訊 2711
政策版本 2711
JSON 政策文件 2711
進一步了解 2714
AWSMarketplaceSellerProductsReadOnly 2715
使用此政策 2715
政策詳細資訊 2715
政策版本 2715
JSON 政策文件 2715
進一步了解 2716
AWSMcpServiceActionsFullAccess 2716
使用此政策 2716
政策詳細資訊 2717
政策版本 2717
JSON 政策文件 2717
進一步了解 2717
AWSMediaConnectServicePolicy 2718
使用此政策 2718
政策詳細資訊 2718
政策版本 2718
JSON 政策文件 2718
進一步了解 2720

AWSMediaLiveAnywhereServiceRolePolicy 2720
使用此政策 2720
政策詳細資訊 2720
政策版本 2721
JSON 政策文件 2721
進一步了解 2724
AWSMediaTailorServiceRolePolicy 2724
使用此政策 2724
政策詳細資訊 2724
政策版本 2724
JSON 政策文件 2725
進一步了解 2725
AWSMigrationHubDiscoveryAccess 2725
使用此政策 2725
政策詳細資訊 2726
政策版本 2726
JSON 政策文件 2726
進一步了解 2727
AWSMigrationHubDMSAccess 2727
使用此政策 2728
政策詳細資訊 2728
政策版本 2728
JSON 政策文件 2728
進一步了解 2729
AWSMigrationHubFullAccess 2729
使用此政策 2729
政策詳細資訊 2729
政策版本 2730
JSON 政策文件 2730
進一步了解 2731
AWSMigrationHubOrchestratorConsoleFullAccess 2731
使用此政策 2732
政策詳細資訊 2732
政策版本 2732
JSON 政策文件 2732
進一步了解 2735

AWSMigrationHubOrchestratorInstanceRolePolicy 2735
使用此政策 2735
政策詳細資訊 2736
政策版本 2736
JSON 政策文件 2736
進一步了解 2737
AWSMigrationHubOrchestratorPlugin 2737
使用此政策 2737
政策詳細資訊 2737
政策版本 2737
JSON 政策文件 2737
進一步了解 2739
AWSMigrationHubOrchestratorServiceRolePolicy 2739
使用此政策 2739
政策詳細資訊 2739
政策版本 2739
JSON 政策文件 2740
進一步了解 2743
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 2743
使用此政策 2743
政策詳細資訊 2744
政策版本 2744
JSON 政策文件 2744
進一步了解 2749
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 2750
使用此政策 2750
政策詳細資訊 2750
政策版本 2750
JSON 政策文件 2750
進一步了解 2752
AWSMigrationHubRefactorSpacesFullAccess 2752
使用此政策 2752
政策詳細資訊 2752
政策版本 2752
JSON 政策文件 2753
進一步了解 2759

AWSMigrationHubRefactorSpacesServiceRolePolicy 2759
使用此政策 2759
政策詳細資訊 2760
政策版本 2760
JSON 政策文件 2760
進一步了解 2764
AWSMigrationHubSMSAccess 2764
使用此政策 2764
政策詳細資訊 2764
政策版本 2764
JSON 政策文件 2764
進一步了解 2765
AWSMigrationHubStrategyCollector 2766
使用此政策 2766
政策詳細資訊 2766
政策版本 2766
JSON 政策文件 2766
進一步了解 2768
AWSMigrationHubStrategyConsoleFullAccess 2769
使用此政策 2769
政策詳細資訊 2769
政策版本 2769
JSON 政策文件 2769
進一步了解 2771
AWSMigrationHubStrategyServiceRolePolicy 2771
使用此政策 2771
政策詳細資訊 2771
政策版本 2772
JSON 政策文件 2772
進一步了解 2773
AWSMobileHub_FullAccess 2773
使用此政策 2773
政策詳細資訊 2773
政策版本 2773
JSON 政策文件 2774
進一步了解 2775

AWSMobileHub_ReadOnly 2775
使用此政策 2775
政策詳細資訊 2776
政策版本 2776
JSON 政策文件 2776
進一步了解 2777
AWSMSKReplicatorExecutionRole 2777
使用此政策 2777
政策詳細資訊 2778
政策版本 2778
JSON 政策文件 2778
進一步了解 2779
AWSNATGatewayServiceRolePolicy 2779
使用此政策 2780
政策詳細資訊 2780
政策版本 2780
JSON 政策文件 2780
進一步了解 2781
AWSNetworkFirewallFullAccess 2781
使用此政策 2781
政策詳細資訊 2781
政策版本 2781
JSON 政策文件 2781
進一步了解 2785
AWSNetworkFirewallReadOnlyAccess 2785
使用此政策 2786
政策詳細資訊 2786
政策版本 2786
JSON 政策文件 2786
進一步了解 2787
AWSNetworkFirewallServiceRolePolicy 2787
使用此政策 2788
政策詳細資訊 2788
政策版本 2788
JSON 政策文件 2788
進一步了解 2790

AWSNetworkManagerCloudWANServiceRolePolicy 2790
使用此政策 2790
政策詳細資訊 2790
政策版本 2790
JSON 政策文件 2790
進一步了解 2791
AWSNetworkManagerFullAccess 2791
使用此政策 2791
政策詳細資訊 2791
政策版本 2791
JSON 政策文件 2792
進一步了解 2792
AWSNetworkManagerReadOnlyAccess 2792
使用此政策 2793
政策詳細資訊 2793
政策版本 2793
JSON 政策文件 2793
進一步了解 2793
AWSNetworkManagerServiceRolePolicy 2794
使用此政策 2794
政策詳細資訊 2794
政策版本 2794
JSON 政策文件 2794
進一步了解 2795
AWSObservabilityAdminLogsCentralizationServiceRolePolicy 2795
使用此政策 2796
政策詳細資訊 2796
政策版本 2796
JSON 政策文件 2796
進一步了解 2797
AWSObservabilityAdminServiceRolePolicy 2797
使用此政策 2797
政策詳細資訊 2797
政策版本 2798
JSON 政策文件 2798
進一步了解 2800

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy 2800
使用此政策 2801
政策詳細資訊 2801
政策版本 2801
JSON 政策文件 2801
進一步了解 2811
AWSOrganizationsFullAccess 2811
使用此政策 2811
政策詳細資訊 2811
政策版本 2812
JSON 政策文件 2812
進一步了解 2813
AWSOrganizationsReadOnlyAccess 2813
使用此政策 2813
政策詳細資訊 2813
政策版本 2813
JSON 政策文件 2814
進一步了解 2814
AWSOrganizationsServiceTrustPolicy 2814
使用此政策 2815
政策詳細資訊 2815
政策版本 2815
JSON 政策文件 2815
進一步了解 2816
AWSOutpostsAuthorizeServerPolicy 2816
使用此政策 2816
政策詳細資訊 2816
政策版本 2816
JSON 政策文件 2817
進一步了解 2817
AWSOutpostsServiceRolePolicy 2817
使用此政策 2817
政策詳細資訊 2818
政策版本 2818
JSON 政策文件 2818
進一步了解 2820

AWSPanoramaApplianceRolePolicy 2820
使用此政策 2820
政策詳細資訊 2820
政策版本 2820
JSON 政策文件 2820
進一步了解 2821
AWSPanoramaApplianceServiceRolePolicy 2821
使用此政策 2821
政策詳細資訊 2822
政策版本 2822
JSON 政策文件 2822
進一步了解 2823
AWSPanoramaFullAccess 2824
使用此政策 2824
政策詳細資訊 2824
政策版本 2824
JSON 政策文件 2824
進一步了解 2827
AWSPanoramaGreengrassGroupRolePolicy 2827
使用此政策 2827
政策詳細資訊 2827
政策版本 2827
JSON 政策文件 2828
進一步了解 2829
AWSPanoramaSageMakerRolePolicy 2829
使用此政策 2829
政策詳細資訊 2829
政策版本 2830
JSON 政策文件 2830
進一步了解 2830
AWSPanoramaServiceLinkedRolePolicy 2830
使用此政策 2831
政策詳細資訊 2831
政策版本 2831
JSON 政策文件 2831
進一步了解 2834

AWSPanoramaServiceRolePolicy 2834
使用此政策 2834
政策詳細資訊 2834
政策版本 2834
JSON 政策文件 2834
進一步了解 2841
AWSPartnerCentralChannelHandshakeApprovalManagement 2842
使用此政策 2842
政策詳細資訊 2842
政策版本 2842
JSON 政策文件 2842
進一步了解 2843
AWSPartnerCentralChannelManagement 2843
使用此政策 2843
政策詳細資訊 2843
政策版本 2844
JSON 政策文件 2844
進一步了解 2847
AWSPartnerCentralFullAccess 2847
使用此政策 2847
政策詳細資訊 2847
政策版本 2847
JSON 政策文件 2847
進一步了解 2852
AWSPartnerCentralMarketingManagement 2852
使用此政策 2852
政策詳細資訊 2852
政策版本 2852
JSON 政策文件 2853
進一步了解 2855
AWSPartnerCentralOpportunityManagement 2855
使用此政策 2855
政策詳細資訊 2856
政策版本 2856
JSON 政策文件 2856
進一步了解 2860

AWSPartnerCentralSandboxFullAccess 2860
使用此政策 2861
政策詳細資訊 2861
政策版本 2861
JSON 政策文件 2861
進一步了解 2862
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 2862
使用此政策 2863
政策詳細資訊 2863
政策版本 2863
JSON 政策文件 2863
進一步了解 2864
AWSPartnerLedSupportReadOnlyAccess 2864
使用此政策 2864
政策詳細資訊 2864
政策版本 2865
JSON 政策文件 2865
進一步了解 2902
AWSPCSComputeNodePolicy 2902
使用此政策 2902
政策詳細資訊 2902
政策版本 2902
JSON 政策文件 2902
進一步了解 2903
AWSPCSServiceRolePolicy 2903
使用此政策 2903
政策詳細資訊 2903
政策版本 2903
JSON 政策文件 2904
進一步了解 2909
AWSPriceListServiceFullAccess 2909
使用此政策 2909
政策詳細資訊 2909
政策版本 2909
JSON 政策文件 2909
進一步了解 2910

AWSPrivateCAAuditor 2910
使用此政策 2910
政策詳細資訊 2910
政策版本 2910
JSON 政策文件 2911
進一步了解 2911
AWSPrivateCAConnectorForKubernetesPolicy 2911
使用此政策 2912
政策詳細資訊 2912
政策版本 2912
JSON 政策文件 2912
進一步了解 2912
AWSPrivateCAFullAccess 2913
使用此政策 2913
政策詳細資訊 2913
政策版本 2913
JSON 政策文件 2913
進一步了解 2914
AWSPrivateCAPrivilegedUser 2914
使用此政策 2914
政策詳細資訊 2914
政策版本 2914
JSON 政策文件 2915
進一步了解 2916
AWSPrivateCAReadOnly 2916
使用此政策 2916
政策詳細資訊 2916
政策版本 2916
JSON 政策文件 2917
進一步了解 2917
AWSPrivateCAUser 2917
使用此政策 2917
政策詳細資訊 2918
政策版本 2918
JSON 政策文件 2918
進一步了解 2919

AWSPrivateMarketplaceAdminFullAccess 2919
使用此政策 2919
政策詳細資訊 2920
政策版本 2920
JSON 政策文件 2920
進一步了解 2923
AWSPrivateMarketplaceRequests 2923
使用此政策 2923
政策詳細資訊 2923
政策版本 2923
JSON 政策文件 2923
進一步了解 2925
AWSPrivateNetworksServiceRolePolicy 2925
使用此政策 2926
政策詳細資訊 2926
政策版本 2926
JSON 政策文件 2926
進一步了解 2927
AWSProtonCodeBuildProvisioningBasicAccess 2927
使用此政策 2927
政策詳細資訊 2927
政策版本 2927
JSON 政策文件 2927
進一步了解 2928
AWSProtonCodeBuildProvisioningServiceRolePolicy 2928
使用此政策 2928
政策詳細資訊 2928
政策版本 2929
JSON 政策文件 2929
進一步了解 2930
AWSProtonDeveloperAccess 2930
使用此政策 2930
政策詳細資訊 2930
政策版本 2931
JSON 政策文件 2931
進一步了解 2933

AWSProtonFullAccess 2933
使用此政策 2933
政策詳細資訊 2934
政策版本 2934
JSON 政策文件 2934
進一步了解 2936
AWSProtonReadOnlyAccess 2936
使用此政策 2936
政策詳細資訊 2936
政策版本 2937
JSON 政策文件 2937
進一步了解 2938
AWSProtonServiceGitSyncServiceRolePolicy 2938
使用此政策 2939
政策詳細資訊 2939
政策版本 2939
JSON 政策文件 2939
進一步了解 2940
AWSProtonSyncServiceRolePolicy 2940
使用此政策 2940
政策詳細資訊 2940
政策版本 2940
JSON 政策文件 2941
進一步了解 2942
AWSPurchaseOrdersServiceRolePolicy 2942
使用此政策 2942
政策詳細資訊 2942
政策版本 2942
JSON 政策文件 2942
進一步了解 2943
AWSQuickSetupCFGCPacksPermissionsBoundary 2944
使用此政策 2944
政策詳細資訊 2944
政策版本 2944
JSON 政策文件 2944
進一步了解 2947

AWSQuickSetupDeploymentRolePolicy 2947
使用此政策 2947
政策詳細資訊 2947
政策版本 2948
JSON 政策文件 2948
進一步了解 2956
AWSQuickSetupDevOpsGuruPermissionsBoundary 2956
使用此政策 2956
政策詳細資訊 2956
政策版本 2957
JSON 政策文件 2957
進一步了解 2960
AWSQuickSetupDistributorPermissionsBoundary 2960
使用此政策 2960
政策詳細資訊 2960
政策版本 2960
JSON 政策文件 2960
進一步了解 2966
AWSQuickSetupEnableAREXExecutionPolicy 2966
使用此政策 2967
政策詳細資訊 2967
政策版本 2967
JSON 政策文件 2967
進一步了解 2969
AWSQuickSetupEnableDHMCExecutionPolicy 2969
使用此政策 2969
政策詳細資訊 2969
政策版本 2969
JSON 政策文件 2969
進一步了解 2971
AWSQuickSetupJITNADeploymentRolePolicy 2971
使用此政策 2971
政策詳細資訊 2971
政策版本 2971
JSON 政策文件 2971
進一步了解 2975

AWSQuickSetupManagedInstanceProfileExecutionPolicy 2975
使用此政策 2975
政策詳細資訊 2975
政策版本 2976
JSON 政策文件 2976
進一步了解 2980
AWSQuickSetupManageJITNAResourcesExecutionPolicy 2980
使用此政策 2980
政策詳細資訊 2980
政策版本 2981
JSON 政策文件 2981
進一步了解 2983
AWSQuickSetupPatchPolicyBaselineAccess 2983
使用此政策 2983
政策詳細資訊 2983
政策版本 2983
JSON 政策文件 2984
進一步了解 2984
AWSQuickSetupPatchPolicyDeploymentRolePolicy 2985
使用此政策 2985
政策詳細資訊 2985
政策版本 2985
JSON 政策文件 2985
進一步了解 2993
AWSQuickSetupPatchPolicyPermissionsBoundary 2993
使用此政策 2993
政策詳細資訊 2994
政策版本 2994
JSON 政策文件 2994
進一步了解 3002
AWSQuickSetupSchedulerPermissionsBoundary 3002
使用此政策 3003
政策詳細資訊 3003
政策版本 3003
JSON 政策文件 3003
進一步了解 3006

AWSQuickSetupSSMDeploymentRolePolicy 3006
使用此政策 3007
政策詳細資訊 3007
政策版本 3007
JSON 政策文件 3007
進一步了解 3018
AWSQuickSetupSSMDeploymentS3BucketRolePolicy 3018
使用此政策 3018
政策詳細資訊 3018
政策版本 3018
JSON 政策文件 3018
進一步了解 3019
AWSQuickSetupSSMHostMgmtPermissionsBoundary 3019
使用此政策 3020
政策詳細資訊 3020
政策版本 3020
JSON 政策文件 3020
進一步了解 3026
AWSQuickSetupSSMLifecycleManagementExecutionPolicy 3026
使用此政策 3026
政策詳細資訊 3026
政策版本 3027
JSON 政策文件 3027
進一步了解 3028
AWSQuickSetupSSMManageResourcesExecutionPolicy 3028
使用此政策 3028
政策詳細資訊 3029
政策版本 3029
JSON 政策文件 3029
進一步了解 3032
AWSQuickSetupStartSSMAssociationsExecutionPolicy 3032
使用此政策 3032
政策詳細資訊 3032
政策版本 3032
JSON 政策文件 3033
進一步了解 3034

AWSQuickSetupStartStopInstancesExecutionPolicy 3034
使用此政策 3034
政策詳細資訊 3034
政策版本 3034
JSON 政策文件 3034
進一步了解 3036
AWSQuickSightAssetBundleExportPolicy 3036
使用此政策 3036
政策詳細資訊 3036
政策版本 3037
JSON 政策文件 3037
進一步了解 3039
AWSQuickSightAssetBundleImportPolicy 3039
使用此政策 3039
政策詳細資訊 3039
政策版本 3040
JSON 政策文件 3040
進一步了解 3043
AWSQuicksightAthenaAccess 3043
使用此政策 3043
政策詳細資訊 3043
政策版本 3043
JSON 政策文件 3043
進一步了解 3046
AWSQuickSightDescribeRDS 3046
使用此政策 3046
政策詳細資訊 3046
政策版本 3046
JSON 政策文件 3046
進一步了解 3047
AWSQuickSightDescribeRedshift 3047
使用此政策 3047
政策詳細資訊 3047
政策版本 3047
JSON 政策文件 3048
進一步了解 3048

AWSQuickSightElasticsearchPolicy 3048
使用此政策 3048
政策詳細資訊 3048
政策版本 3049
JSON 政策文件 3049
進一步了解 3050
AWSQuickSightIoTAnalyticsAccess 3050
使用此政策 3050
政策詳細資訊 3050
政策版本 3051
JSON 政策文件 3051
進一步了解 3051
AWSQuickSightListIAM 3051
使用此政策 3052
政策詳細資訊 3052
政策版本 3052
JSON 政策文件 3052
進一步了解 3052
AWSQuicksightOpenSearchPolicy 3053
使用此政策 3053
政策詳細資訊 3053
政策版本 3053
JSON 政策文件 3053
進一步了解 3054
AWSQuickSightSageMakerPolicy 3054
使用此政策 3055
政策詳細資訊 3055
政策版本 3055
JSON 政策文件 3055
進一步了解 3056
AWSQuickSightSecretsManagerWriteAccess 3057
使用此政策 3057
政策詳細資訊 3057
政策版本 3057
JSON 政策文件 3057
進一步了解 3058

AWSQuickSightSecretsManagerWritePolicy 3058
使用此政策 3058
政策詳細資訊 3059
政策版本 3059
JSON 政策文件 3059
進一步了解 3060
AWSQuickSightTimestreamPolicy 3060
使用此政策 3060
政策詳細資訊 3060
政策版本 3060
JSON 政策文件 3061
進一步了解 3061
AWSReachabilityAnalyzerServiceRolePolicy 3061
使用此政策 3062
政策詳細資訊 3062
政策版本 3062
JSON 政策文件 3062
進一步了解 3064
AWSRefactoringToolkitFullAccess 3064
使用此政策 3065
政策詳細資訊 3065
政策版本 3065
JSON 政策文件 3065
進一步了解 3079
AWSRefactoringToolkitSidecarPolicy 3079
使用此政策 3079
政策詳細資訊 3079
政策版本 3079
JSON 政策文件 3080
進一步了解 3081
AWSrePostPrivateCloudWatchAccess 3081
使用此政策 3081
政策詳細資訊 3081
政策版本 3081
JSON 政策文件 3081
進一步了解 3082

AWSRepostSpaceSupportOperationsPolicy 3082
使用此政策 3082
政策詳細資訊 3082
政策版本 3083
JSON 政策文件 3083
進一步了解 3083
AWSResilienceHubAsssessmentExecutionPolicy 3084
使用此政策 3084
政策詳細資訊 3084
政策版本 3084
JSON 政策文件 3084
進一步了解 3089
AWSResourceAccessManagerFullAccess 3089
使用此政策 3089
政策詳細資訊 3089
政策版本 3090
JSON 政策文件 3090
進一步了解 3090
AWSResourceAccessManagerReadOnlyAccess 3090
使用此政策 3090
政策詳細資訊 3091
政策版本 3091
JSON 政策文件 3091
進一步了解 3091
AWSResourceAccessManagerResourceShareParticipantAccess 3092
使用此政策 3092
政策詳細資訊 3092
政策版本 3092
JSON 政策文件 3092
進一步了解 3093
AWSResourceAccessManagerServiceRolePolicy 3093
使用此政策 3093
政策詳細資訊 3093
政策版本 3093
JSON 政策文件 3094
進一步了解 3094

AWSResourceExplorerFullAccess 3095
使用此政策 3095
政策詳細資訊 3095
政策版本 3095
JSON 政策文件 3095
進一步了解 3096
AWSResourceExplorerOrganizationsAccess 3096
使用此政策 3096
政策詳細資訊 3097
政策版本 3097
JSON 政策文件 3097
進一步了解 3099
AWSResourceExplorerReadOnlyAccess 3099
使用此政策 3099
政策詳細資訊 3099
政策版本 3099
JSON 政策文件 3099
進一步了解 3100
AWSResourceExplorerServiceRolePolicy 3100
使用此政策 3100
政策詳細資訊 3100
政策版本 3101
JSON 政策文件 3101
進一步了解 3122
AWSResourceGroupsReadOnlyAccess 3122
使用此政策 3122
政策詳細資訊 3122
政策版本 3122
JSON 政策文件 3123
進一步了解 3124
AWSRoboMaker_FullAccess 3124
使用此政策 3124
政策詳細資訊 3124
政策版本 3125
JSON 政策文件 3125
進一步了解 3126

AWSRoboMakerReadOnlyAccess 3126
使用此政策 3126
政策詳細資訊 3126
政策版本 3127
JSON 政策文件 3127
進一步了解 3127
AWSRoboMakerServicePolicy 3127
使用此政策 3128
政策詳細資訊 3128
政策版本 3128
JSON 政策文件 3128
進一步了解 3130
AWSRoboMakerServiceRolePolicy 3130
使用此政策 3130
政策詳細資訊 3130
政策版本 3130
JSON 政策文件 3130
進一步了解 3132
AWSRolesAnywhereFullAccess 3132
使用此政策 3132
政策詳細資訊 3132
政策版本 3132
JSON 政策文件 3132
進一步了解 3135
AWSRolesAnywhereReadOnly 3135
使用此政策 3135
政策詳細資訊 3135
政策版本 3136
JSON 政策文件 3136
進一步了解 3137
AWSRolesAnywhereServicePolicy 3137
使用此政策 3138
政策詳細資訊 3138
政策版本 3138
JSON 政策文件 3138
進一步了解 3139

AWSS3OnOutpostsServiceRolePolicy 3139
使用此政策 3139
政策詳細資訊 3139
政策版本 3139
JSON 政策文件 3140
進一步了解 3142
AWSSavingsPlansFullAccess 3142
使用此政策 3143
政策詳細資訊 3143
政策版本 3143
JSON 政策文件 3143
進一步了解 3143
AWSSavingsPlansReadOnlyAccess 3144
使用此政策 3144
政策詳細資訊 3144
政策版本 3144
JSON 政策文件 3144
進一步了解 3145
AWSSecretsManagerClientReadOnlyAccess 3145
使用此政策 3145
政策詳細資訊 3145
政策版本 3145
JSON 政策文件 3145
進一步了解 3146
AWSSecurityAgentWebAppPolicy 3146
使用此政策 3147
政策詳細資訊 3147
政策版本 3147
JSON 政策文件 3147
進一步了解 3149
AWSSecurityHubFullAccess 3149
使用此政策 3149
政策詳細資訊 3149
政策版本 3149
JSON 政策文件 3149
進一步了解 3151

AWSSecurityHubOrganizationsAccess 3151
使用此政策 3151
政策詳細資訊 3151
政策版本 3151
JSON 政策文件 3152
進一步了解 3154
AWSSecurityHubReadOnlyAccess 3154
使用此政策 3154
政策詳細資訊 3155
政策版本 3155
JSON 政策文件 3155
進一步了解 3155
AWSSecurityHubServiceRolePolicy 3156
使用此政策 3156
政策詳細資訊 3156
政策版本 3156
JSON 政策文件 3156
進一步了解 3158
AWSSecurityHubV2ServiceRolePolicy 3158
使用此政策 3159
政策詳細資訊 3159
政策版本 3159
JSON 政策文件 3159
進一步了解 3162
AWSSecurityIncidentResponseCaseFullAccess 3162
使用此政策 3162
政策詳細資訊 3162
政策版本 3163
JSON 政策文件 3163
進一步了解 3164
AWSSecurityIncidentResponseFullAccess 3164
使用此政策 3165
政策詳細資訊 3165
政策版本 3165
JSON 政策文件 3165
進一步了解 3167

AWSSecurityIncidentResponseReadOnlyAccess 3167
使用此政策 3168
政策詳細資訊 3168
政策版本 3168
JSON 政策文件 3168
進一步了解 3169
AWSSecurityIncidentResponseServiceRolePolicy 3169
使用此政策 3169
政策詳細資訊 3169
政策版本 3169
JSON 政策文件 3170
進一步了解 3171
AWSSecurityIncidentResponseTriageServiceRolePolicy 3171
使用此政策 3171
政策詳細資訊 3171
政策版本 3172
JSON 政策文件 3172
進一步了解 3174
AWSServiceCatalogAdminFullAccess 3174
使用此政策 3174
政策詳細資訊 3174
政策版本 3175
JSON 政策文件 3175
進一步了解 3177
AWSServiceCatalogAdminReadOnlyAccess 3178
使用此政策 3178
政策詳細資訊 3178
政策版本 3178
JSON 政策文件 3178
進一步了解 3179
AWSServiceCatalogAppRegistryFullAccess 3180
使用此政策 3180
政策詳細資訊 3180
政策版本 3180
JSON 政策文件 3180
進一步了解 3182

AWSServiceCatalogAppRegistryReadOnlyAccess 3183
使用此政策 3183
政策詳細資訊 3183
政策版本 3183
JSON 政策文件 3183
進一步了解 3184
AWSServiceCatalogAppRegistryServiceRolePolicy 3184
使用此政策 3184
政策詳細資訊 3184
政策版本 3185
JSON 政策文件 3185
進一步了解 3186
AWSServiceCatalogEndUserFullAccess 3186
使用此政策 3186
政策詳細資訊 3186
政策版本 3187
JSON 政策文件 3187
進一步了解 3189
AWSServiceCatalogEndUserReadOnlyAccess 3189
使用此政策 3189
政策詳細資訊 3189
政策版本 3189
JSON 政策文件 3190
進一步了解 3191
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 3191
使用此政策 3192
政策詳細資訊 3192
政策版本 3192
JSON 政策文件 3192
進一步了解 3193
AWSServiceCatalogSyncServiceRolePolicy 3193
使用此政策 3193
政策詳細資訊 3193
政策版本 3194
JSON 政策文件 3194
進一步了解 3195

AWSServiceRoleForAIDevOpsPolicy 3195
使用此政策 3195
政策詳細資訊 3195
政策版本 3195
JSON 政策文件 3196
進一步了解 3196
AWSServiceRoleForAmazonEKSNodegroup 3196
使用此政策 3196
政策詳細資訊 3197
政策版本 3197
JSON 政策文件 3197
進一步了解 3203
AWSServiceRoleForAmazonQDeveloper 3203
使用此政策 3203
政策詳細資訊 3203
政策版本 3203
JSON 政策文件 3203
進一步了解 3204
AWSServiceRoleForAWSTransform 3204
使用此政策 3204
政策詳細資訊 3204
政策版本 3205
JSON 政策文件 3205
進一步了解 3207
AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 3207
使用此政策 3207
政策詳細資訊 3207
政策版本 3208
JSON 政策文件 3208
進一步了解 3208
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 3208
使用此政策 3208
政策詳細資訊 3209
政策版本 3209
JSON 政策文件 3209
進一步了解 3209

AWSServiceRoleForCodeGuru-Profiler 3210
使用此政策 3210
政策詳細資訊 3210
政策版本 3210
JSON 政策文件 3210
進一步了解 3211
AWSServiceRoleForCodeWhispererPolicy 3211
使用此政策 3211
政策詳細資訊 3211
政策版本 3211
JSON 政策文件 3211
進一步了解 3213
AWSServiceRoleForEC2ScheduledInstances 3213
使用此政策 3213
政策詳細資訊 3214
政策版本 3214
JSON 政策文件 3214
進一步了解 3215
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 3215
使用此政策 3215
政策詳細資訊 3215
政策版本 3215
JSON 政策文件 3216
進一步了解 3216
AWSServiceRoleForImageBuilder 3216
使用此政策 3216
政策詳細資訊 3216
政策版本 3217
JSON 政策文件 3217
進一步了解 3228
AWSServiceRoleForIoTSiteWise 3228
使用此政策 3228
政策詳細資訊 3228
政策版本 3228
JSON 政策文件 3228
進一步了解 3230

AWSServiceRoleForLogDeliveryPolicy 3230
使用此政策 3230
政策詳細資訊 3230
政策版本 3230
JSON 政策文件 3231
進一步了解 3231
AWSServiceRoleForMonitronPolicy 3231
使用此政策 3231
政策詳細資訊 3232
政策版本 3232
JSON 政策文件 3232
進一步了解 3233
AWSServiceRoleForNeptuneGraphPolicy 3233
使用此政策 3234
政策詳細資訊 3234
政策版本 3234
JSON 政策文件 3234
進一步了解 3235
AWSServiceRoleForPrivateMarketplaceAdminPolicy 3236
使用此政策 3236
政策詳細資訊 3236
政策版本 3236
JSON 政策文件 3236
進一步了解 3238
AWSServiceRoleForProcurementInsightsPolicy 3238
使用此政策 3238
政策詳細資訊 3238
政策版本 3239
JSON 政策文件 3239
進一步了解 3239
AWSServiceRoleForSMS 3239
使用此政策 3240
政策詳細資訊 3240
政策版本 3240
JSON 政策文件 3240
進一步了解 3247

AWSServiceRoleForUserSubscriptions 3247
使用此政策 3247
政策詳細資訊 3247
政策版本 3247
JSON 政策文件 3248
進一步了解 3249
AWSServiceRolePolicyForBackupReports 3249
使用此政策 3249
政策詳細資訊 3249
政策版本 3250
JSON 政策文件 3250
進一步了解 3251
AWSServiceRolePolicyForBackupRestoreTesting 3251
使用此政策 3251
政策詳細資訊 3251
政策版本 3252
JSON 政策文件 3252
進一步了解 3255
AWSServiceRolePolicyForWorkspacesInstances 3255
使用此政策 3255
政策詳細資訊 3255
政策版本 3255
JSON 政策文件 3255
進一步了解 3256
AWSShieldDRTAccessPolicy 3256
使用此政策 3256
政策詳細資訊 3257
政策版本 3257
JSON 政策文件 3257
進一步了解 3258
AWSShieldServiceRolePolicy 3258
使用此政策 3258
政策詳細資訊 3258
政策版本 3259
JSON 政策文件 3259
進一步了解 3259

AWSSocialMessagingServiceRolePolicy 3259
使用此政策 3260
政策詳細資訊 3260
政策版本 3260
JSON 政策文件 3260
進一步了解 3261
AWSSSMForSAPServiceLinkedRolePolicy 3261
使用此政策 3261
政策詳細資訊 3261
政策版本 3261
JSON 政策文件 3261
進一步了解 3270
AWSSSMOpsInsightsServiceRolePolicy 3270
使用此政策 3270
政策詳細資訊 3270
政策版本 3270
JSON 政策文件 3271
進一步了解 3271
AWSSSODirectoryAdministrator 3272
使用此政策 3272
政策詳細資訊 3272
政策版本 3272
JSON 政策文件 3272
進一步了解 3273
AWSSSODirectoryReadOnly 3273
使用此政策 3273
政策詳細資訊 3273
政策版本 3274
JSON 政策文件 3274
進一步了解 3275
AWSSSOMasterAccountAdministrator 3275
使用此政策 3275
政策詳細資訊 3275
政策版本 3275
JSON 政策文件 3276
進一步了解 3278

AWSSSOMemberAccountAdministrator 3279
使用此政策 3279
政策詳細資訊 3279
政策版本 3279
JSON 政策文件 3279
進一步了解 3281
AWSSSOReadOnly 3282
使用此政策 3282
政策詳細資訊 3282
政策版本 3282
JSON 政策文件 3282
進一步了解 3284
AWSSSOServiceRolePolicy 3284
使用此政策 3284
政策詳細資訊 3284
政策版本 3284
JSON 政策文件 3284
進一步了解 3288
AWSStepFunctionsConsoleFullAccess 3288
使用此政策 3288
政策詳細資訊 3289
政策版本 3289
JSON 政策文件 3289
進一步了解 3290
AWSStepFunctionsFullAccess 3290
使用此政策 3290
政策詳細資訊 3290
政策版本 3290
JSON 政策文件 3290
進一步了解 3291
AWSStepFunctionsReadOnlyAccess 3291
使用此政策 3291
政策詳細資訊 3291
政策版本 3291
JSON 政策文件 3292
進一步了解 3292

AWSStorageGatewayFullAccess 3293
使用此政策 3293
政策詳細資訊 3293
政策版本 3293
JSON 政策文件 3293
進一步了解 3294
AWSStorageGatewayReadOnlyAccess 3294
使用此政策 3294
政策詳細資訊 3294
政策版本 3295
JSON 政策文件 3295
進一步了解 3295
AWSStorageGatewayServiceRolePolicy 3296
使用此政策 3296
政策詳細資訊 3296
政策版本 3296
JSON 政策文件 3296
進一步了解 3297
AWSSupplyChainFederationAdminAccess 3297
使用此政策 3297
政策詳細資訊 3297
政策版本 3297
JSON 政策文件 3298
進一步了解 3304
AWSSupportAccess 3304
使用此政策 3304
政策詳細資訊 3304
政策版本 3304
JSON 政策文件 3304
進一步了解 3305
AWSSupportAppFullAccess 3305
使用此政策 3305
政策詳細資訊 3305
政策版本 3306
JSON 政策文件 3306
進一步了解 3307

AWSSupportAppReadOnlyAccess 3307
使用此政策 3307
政策詳細資訊 3307
政策版本 3307
JSON 政策文件 3307
進一步了解 3308
AWSSupportPlansFullAccess 3308
使用此政策 3308
政策詳細資訊 3308
政策版本 3308
JSON 政策文件 3309
進一步了解 3309
AWSSupportPlansReadOnlyAccess 3309
使用此政策 3309
政策詳細資訊 3310
政策版本 3310
JSON 政策文件 3310
進一步了解 3310
AWSSupportServiceRolePolicy 3311
使用此政策 3311
政策詳細資訊 3311
政策版本 3311
JSON 政策文件 3311
進一步了解 3406
AWSSystemsManagerAccountDiscoveryServicePolicy 3406
使用此政策 3406
政策詳細資訊 3406
政策版本 3406
JSON 政策文件 3407
進一步了解 3407
AWSSystemsManagerChangeManagementServicePolicy 3407
使用此政策 3407
政策詳細資訊 3408
政策版本 3408
JSON 政策文件 3408
進一步了解 3410

AWSSystemsManagerEnableConfigRecordingExecutionPolicy 3411
使用此政策 3411
政策詳細資訊 3411
政策版本 3411
JSON 政策文件 3411
進一步了解 3413
AWSSystemsManagerEnableExplorerExecutionPolicy 3413
使用此政策 3414
政策詳細資訊 3414
政策版本 3414
JSON 政策文件 3414
進一步了解 3415
AWSSystemsManagerForSAPFullAccess 3416
使用此政策 3416
政策詳細資訊 3416
政策版本 3416
JSON 政策文件 3416
進一步了解 3417
AWSSystemsManagerForSAPReadOnlyAccess 3417
使用此政策 3418
政策詳細資訊 3418
政策版本 3418
JSON 政策文件 3418
進一步了解 3418
AWSSystemsManagerJustInTimeAccessServicePolicy 3419
使用此政策 3419
政策詳細資訊 3419
政策版本 3419
JSON 政策文件 3419
進一步了解 3425
AWSSystemsManagerJustInTimeAccessTokenPolicy 3425
使用此政策 3425
政策詳細資訊 3425
政策版本 3425
JSON 政策文件 3425
進一步了解 3428

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 3428
使用此政策 3429
政策詳細資訊 3429
政策版本 3429
JSON 政策文件 3429
進一步了解 3432
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 3432
使用此政策 3432
政策詳細資訊 3432
政策版本 3432
JSON 政策文件 3432
進一步了解 3437
AWSSystemsManagerNotificationsServicePolicy 3437
使用此政策 3437
政策詳細資訊 3437
政策版本 3437
JSON 政策文件 3437
進一步了解 3439
AWSSystemsManagerOpsDataSyncServiceRolePolicy 3439
使用此政策 3439
政策詳細資訊 3439
政策版本 3439
JSON 政策文件 3440
進一步了解 3443
AWSThinkboxAssetServerPolicy 3443
使用此政策 3443
政策詳細資訊 3444
政策版本 3444
JSON 政策文件 3444
進一步了解 3445
AWSThinkboxAWSPortalAdminPolicy 3445
使用此政策 3445
政策詳細資訊 3445
政策版本 3445
JSON 政策文件 3446
進一步了解 3455

AWSThinkboxAWSPortalGatewayPolicy 3456
使用此政策 3456
政策詳細資訊 3456
政策版本 3456
JSON 政策文件 3456
進一步了解 3458
AWSThinkboxAWSPortalWorkerPolicy 3458
使用此政策 3458
政策詳細資訊 3458
政策版本 3459
JSON 政策文件 3459
進一步了解 3461
AWSThinkboxDeadlineResourceTrackerAccessPolicy 3461
使用此政策 3461
政策詳細資訊 3461
政策版本 3461
JSON 政策文件 3462
進一步了解 3464
AWSThinkboxDeadlineResourceTrackerAdminPolicy 3464
使用此政策 3465
政策詳細資訊 3465
政策版本 3465
JSON 政策文件 3465
進一步了解 3471
AWSThinkboxDeadlineSpotEventPluginAdminPolicy 3471
使用此政策 3471
政策詳細資訊 3471
政策版本 3472
JSON 政策文件 3472
進一步了解 3474
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 3475
使用此政策 3475
政策詳細資訊 3475
政策版本 3475
JSON 政策文件 3475
進一步了解 3477

AWSTransferConsoleFullAccess 3477
使用此政策 3477
政策詳細資訊 3477
政策版本 3477
JSON 政策文件 3477
進一步了解 3478
AWSTransferFullAccess 3479
使用此政策 3479
政策詳細資訊 3479
政策版本 3479
JSON 政策文件 3479
進一步了解 3480
AWSTransferLoggingAccess 3480
使用此政策 3480
政策詳細資訊 3480
政策版本 3481
JSON 政策文件 3481
進一步了解 3481
AWSTransferReadOnlyAccess 3481
使用此政策 3482
政策詳細資訊 3482
政策版本 3482
JSON 政策文件 3482
進一步了解 3483
AWSTransformApplicationDeploymentPolicy 3483
使用此政策 3483
政策詳細資訊 3483
政策版本 3483
JSON 政策文件 3483
進一步了解 3491
AWSTransformApplicationECSDeploymentPolicy 3492
使用此政策 3492
政策詳細資訊 3492
政策版本 3492
JSON 政策文件 3492
進一步了解 3500

AWSTransformCustomExecuteTransformations 3500
使用此政策 3500
政策詳細資訊 3501
政策版本 3501
JSON 政策文件 3501
進一步了解 3501
AWSTransformCustomFullAccess 3502
使用此政策 3502
政策詳細資訊 3502
政策版本 3502
JSON 政策文件 3502
進一步了解 3503
AWSTransformCustomManageTransformations 3503
使用此政策 3503
政策詳細資訊 3503
政策版本 3503
JSON 政策文件 3504
進一步了解 3504
AWSTransformSecretsManagerConnectorPolicy 3505
使用此政策 3505
政策詳細資訊 3505
政策版本 3505
JSON 政策文件 3505
進一步了解 3506
AWSTrustedAdvisorPriorityFullAccess 3507
使用此政策 3507
政策詳細資訊 3507
政策版本 3507
JSON 政策文件 3507
進一步了解 3509
AWSTrustedAdvisorPriorityReadOnlyAccess 3509
使用此政策 3509
政策詳細資訊 3509
政策版本 3510
JSON 政策文件 3510
進一步了解 3511

AWSTrustedAdvisorReportingServiceRolePolicy 3511
使用此政策 3511
政策詳細資訊 3511
政策版本 3511
JSON 政策文件 3512
進一步了解 3512
AWSTrustedAdvisorServiceRolePolicy 3512
使用此政策 3512
政策詳細資訊 3513
政策版本 3513
JSON 政策文件 3513
進一步了解 3516
AWSUserAttributeCostAllocationPolicy 3516
使用此政策 3516
政策詳細資訊 3516
政策版本 3517
JSON 政策文件 3517
進一步了解 3517
AWSUserNotificationsServiceLinkedRolePolicy 3517
使用此政策 3517
政策詳細資訊 3517
政策版本 3518
JSON 政策文件 3518
進一步了解 3520
AWSVendorInsightsAssessorFullAccess 3520
使用此政策 3520
政策詳細資訊 3520
政策版本 3520
JSON 政策文件 3520
進一步了解 3521
AWSVendorInsightsAssessorReadOnly 3522
使用此政策 3522
政策詳細資訊 3522
政策版本 3522
JSON 政策文件 3522
進一步了解 3523

AWSVendorInsightsVendorFullAccess 3523
使用此政策 3523
政策詳細資訊 3523
政策版本 3524
JSON 政策文件 3524
進一步了解 3525
AWSVendorInsightsVendorReadOnly 3526
使用此政策 3526
政策詳細資訊 3526
政策版本 3526
JSON 政策文件 3526
進一步了解 3527
AWSVpcLatticeServiceRolePolicy 3527
使用此政策 3528
政策詳細資訊 3528
政策版本 3528
JSON 政策文件 3528
進一步了解 3531
AWSVPCS2SVpnServiceRolePolicy 3531
使用此政策 3531
政策詳細資訊 3531
政策版本 3531
JSON 政策文件 3532
進一步了解 3533
AWSVPCTransitGatewayServiceRolePolicy 3533
使用此政策 3533
政策詳細資訊 3533
政策版本 3533
JSON 政策文件 3534
進一步了解 3534
AWSVPCVerifiedAccessServiceRolePolicy 3534
使用此政策 3534
政策詳細資訊 3535
政策版本 3535
JSON 政策文件 3535
進一步了解 3537

AWSWAFConsoleFullAccess 3537
使用此政策 3537
政策詳細資訊 3537
政策版本 3537
JSON 政策文件 3537
進一步了解 3546
AWSWAFConsoleReadOnlyAccess 3546
使用此政策 3546
政策詳細資訊 3546
政策版本 3547
JSON 政策文件 3547
進一步了解 3553
AWSWAFFullAccess 3554
使用此政策 3554
政策詳細資訊 3554
政策版本 3554
JSON 政策文件 3554
進一步了解 3559
AWSWAFReadOnlyAccess 3559
使用此政策 3560
政策詳細資訊 3560
政策版本 3560
JSON 政策文件 3560
進一步了解 3563
AWSWellArchitectedDiscoveryServiceRolePolicy 3563
使用此政策 3564
政策詳細資訊 3564
政策版本 3564
JSON 政策文件 3564
進一步了解 3566
AWSWellArchitectedOrganizationsServiceRolePolicy 3566
使用此政策 3566
政策詳細資訊 3566
政策版本 3566
JSON 政策文件 3566
進一步了解 3567

AWSWickrFullAccess 3567
使用此政策 3567
政策詳細資訊 3567
政策版本 3567
JSON 政策文件 3568
進一步了解 3568
AWSXrayCrossAccountSharingConfiguration 3568
使用此政策 3568
政策詳細資訊 3568
政策版本 3569
JSON 政策文件 3569
進一步了解 3570
AWSXRayDaemonWriteAccess 3570
使用此政策 3570
政策詳細資訊 3570
政策版本 3570
JSON 政策文件 3571
進一步了解 3571
AWSXrayFullAccess 3571
使用此政策 3571
政策詳細資訊 3572
政策版本 3572
JSON 政策文件 3572
進一步了解 3572
AWSXrayReadOnlyAccess 3573
使用此政策 3573
政策詳細資訊 3573
政策版本 3573
JSON 政策文件 3573
進一步了解 3574
AWSXrayWriteOnlyAccess 3574
使用此政策 3574
政策詳細資訊 3574
政策版本 3575
JSON 政策文件 3575
進一步了解 3575

AWSZonalAutoshiftPracticeRunSLRPolicy 3576
使用此政策 3576
政策詳細資訊 3576
政策版本 3576
JSON 政策文件 3576
進一步了解 3577
AWSZoneGroupAccessManagementServiceRolePolicy 3577
使用此政策 3577
政策詳細資訊 3578
政策版本 3578
JSON 政策文件 3578
進一步了解 3579
BatchServiceRolePolicy 3579
使用此政策 3579
政策詳細資訊 3579
政策版本 3579
JSON 政策文件 3579
進一步了解 3585
BedrockAgentCoreFullAccess 3586
使用此政策 3586
政策詳細資訊 3586
政策版本 3586
JSON 政策文件 3586
進一步了解 3595
BedrockAgentCoreNetworkServiceRolePolicy 3595
使用此政策 3596
政策詳細資訊 3596
政策版本 3596
JSON 政策文件 3596
進一步了解 3598
BedrockAgentCoreRuntimeIdentityServiceRolePolicy 3598
使用此政策 3598
政策詳細資訊 3598
政策版本 3599
JSON 政策文件 3599
進一步了解 3599

Billing 3599
使用此政策 3600
政策詳細資訊 3600
政策版本 3600
JSON 政策文件 3600
進一步了解 3604
BudgetsServiceRolePolicy 3604
使用此政策 3604
政策詳細資訊 3604
政策版本 3604
JSON 政策文件 3605
進一步了解 3605
CertificateManagerServiceRolePolicy 3605
使用此政策 3605
政策詳細資訊 3605
政策版本 3606
JSON 政策文件 3606
進一步了解 3606
ClientVPNServiceConnectionsRolePolicy 3606
使用此政策 3606
政策詳細資訊 3607
政策版本 3607
JSON 政策文件 3607
進一步了解 3607
ClientVPNServiceRolePolicy 3607
使用此政策 3608
政策詳細資訊 3608
政策版本 3608
JSON 政策文件 3608
進一步了解 3609
CloudFormationStackSetsOrgAdminServiceRolePolicy 3609
使用此政策 3609
政策詳細資訊 3609
政策版本 3610
JSON 政策文件 3610
進一步了解 3610

CloudFormationStackSetsOrgMemberServiceRolePolicy 3610
使用此政策 3611
政策詳細資訊 3611
政策版本 3611
JSON 政策文件 3611
進一步了解 3612
CloudFrontFullAccess 3612
使用此政策 3612
政策詳細資訊 3612
政策版本 3613
JSON 政策文件 3613
進一步了解 3615
CloudFrontReadOnlyAccess 3615
使用此政策 3615
政策詳細資訊 3615
政策版本 3615
JSON 政策文件 3615
進一步了解 3616
CloudHSMServiceRolePolicy 3616
使用此政策 3617
政策詳細資訊 3617
政策版本 3617
JSON 政策文件 3617
進一步了解 3618
CloudSearchFullAccess 3618
使用此政策 3618
政策詳細資訊 3618
政策版本 3618
JSON 政策文件 3618
進一步了解 3619
CloudSearchReadOnlyAccess 3619
使用此政策 3619
政策詳細資訊 3619
政策版本 3619
JSON 政策文件 3620
進一步了解 3620

CloudTrailEventContext 3620
使用此政策 3620
政策詳細資訊 3620
政策版本 3621
JSON 政策文件 3621
進一步了解 3622
CloudTrailServiceRolePolicy 3623
使用此政策 3623
政策詳細資訊 3623
政策版本 3623
JSON 政策文件 3623
進一步了解 3625
CloudWatch-CrossAccountAccess 3625
使用此政策 3625
政策詳細資訊 3625
政策版本 3626
JSON 政策文件 3626
進一步了解 3626
CloudWatchActionsEC2Access 3626
使用此政策 3626
政策詳細資訊 3627
政策版本 3627
JSON 政策文件 3627
進一步了解 3627
CloudWatchAgentAdminPolicy 3628
使用此政策 3628
政策詳細資訊 3628
政策版本 3628
JSON 政策文件 3628
進一步了解 3629
CloudWatchAgentServerPolicy 3629
使用此政策 3629
政策詳細資訊 3630
政策版本 3630
JSON 政策文件 3630
進一步了解 3631

CloudWatchApplicationInsightsFullAccess 3631
使用此政策 3631
政策詳細資訊 3631
政策版本 3631
JSON 政策文件 3632
進一步了解 3633
CloudWatchApplicationInsightsReadOnlyAccess 3633
使用此政策 3633
政策詳細資訊 3633
政策版本 3634
JSON 政策文件 3634
進一步了解 3634
CloudwatchApplicationInsightsServiceLinkedRolePolicy 3634
使用此政策 3635
政策詳細資訊 3635
政策版本 3635
JSON 政策文件 3635
進一步了解 3646
CloudWatchApplicationSignalsFullAccess 3646
使用此政策 3646
政策詳細資訊 3646
政策版本 3646
JSON 政策文件 3646
進一步了解 3652
CloudWatchApplicationSignalsReadOnlyAccess 3652
使用此政策 3652
政策詳細資訊 3652
政策版本 3652
JSON 政策文件 3652
進一步了解 3656
CloudWatchApplicationSignalsServiceRolePolicy 3657
使用此政策 3657
政策詳細資訊 3657
政策版本 3657
JSON 政策文件 3657
進一步了解 3660

CloudWatchAutomaticDashboardsAccess 3661
使用此政策 3661
政策詳細資訊 3661
政策版本 3661
JSON 政策文件 3661
進一步了解 3663
CloudWatchCrossAccountSharingConfiguration 3663
使用此政策 3663
政策詳細資訊 3663
政策版本 3663
JSON 政策文件 3663
進一步了解 3664
CloudWatchEventsBuiltInTargetExecutionAccess 3664
使用此政策 3665
政策詳細資訊 3665
政策版本 3665
JSON 政策文件 3665
進一步了解 3666
CloudWatchEventsFullAccess 3666
使用此政策 3666
政策詳細資訊 3666
政策版本 3666
JSON 政策文件 3666
進一步了解 3668
CloudWatchEventsInvocationAccess 3669
使用此政策 3669
政策詳細資訊 3669
政策版本 3669
JSON 政策文件 3669
進一步了解 3670
CloudWatchEventsReadOnlyAccess 3670
使用此政策 3670
政策詳細資訊 3670
政策版本 3670
JSON 政策文件 3670
進一步了解 3672

CloudWatchEventsServiceRolePolicy 3672
使用此政策 3672
政策詳細資訊 3672
政策版本 3672
JSON 政策文件 3673
進一步了解 3673
CloudWatchFullAccess 3673
使用此政策 3673
政策詳細資訊 3674
政策版本 3674
JSON 政策文件 3674
進一步了解 3675
CloudWatchFullAccessV2 3675
使用此政策 3675
政策詳細資訊 3675
政策版本 3676
JSON 政策文件 3676
進一步了解 3681
CloudWatchInternetMonitorFullAccess 3681
使用此政策 3681
政策詳細資訊 3681
政策版本 3682
JSON 政策文件 3682
進一步了解 3684
CloudWatchInternetMonitorReadOnlyAccess 3684
使用此政策 3684
政策詳細資訊 3684
政策版本 3684
JSON 政策文件 3685
進一步了解 3685
CloudWatchInternetMonitorServiceRolePolicy 3686
使用此政策 3686
政策詳細資訊 3686
政策版本 3686
JSON 政策文件 3686
進一步了解 3687

CloudWatchLambdaApplicationSignalsExecutionRolePolicy 3687
使用此政策 3688
政策詳細資訊 3688
政策版本 3688
JSON 政策文件 3688
進一步了解 3689
CloudWatchLambdaInsightsExecutionRolePolicy 3689
使用此政策 3689
政策詳細資訊 3689
政策版本 3690
JSON 政策文件 3690
進一步了解 3690
CloudWatchLogsAPIKeyAccess 3691
使用此政策 3691
政策詳細資訊 3691
政策版本 3691
JSON 政策文件 3691
進一步了解 3692
CloudWatchLogsCrossAccountSharingConfiguration 3692
使用此政策 3693
政策詳細資訊 3693
政策版本 3693
JSON 政策文件 3693
進一步了解 3694
CloudWatchLogsFullAccess 3694
使用此政策 3694
政策詳細資訊 3694
政策版本 3695
JSON 政策文件 3695
進一步了解 3695
CloudWatchLogsReadOnlyAccess 3696
使用此政策 3696
政策詳細資訊 3696
政策版本 3696
JSON 政策文件 3696
進一步了解 3697

CloudWatchNetworkFlowMonitorAgentPublishPolicy 3697
使用此政策 3697
政策詳細資訊 3697
政策版本 3698
JSON 政策文件 3698
進一步了解 3698
CloudWatchNetworkFlowMonitorServiceRolePolicy 3698
使用此政策 3699
政策詳細資訊 3699
政策版本 3699
JSON 政策文件 3699
進一步了解 3700
CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy 3700
使用此政策 3700
政策詳細資訊 3700
政策版本 3701
JSON 政策文件 3701
進一步了解 3702
CloudWatchNetworkMonitorServiceRolePolicy 3702
使用此政策 3702
政策詳細資訊 3702
政策版本 3703
JSON 政策文件 3703
進一步了解 3704
CloudWatchOpenSearchDashboardAccess 3704
使用此政策 3704
政策詳細資訊 3704
政策版本 3705
JSON 政策文件 3705
進一步了解 3707
CloudWatchOpenSearchDashboardsFullAccess 3707
使用此政策 3708
政策詳細資訊 3708
政策版本 3708
JSON 政策文件 3708
進一步了解 3715

CloudWatchReadOnlyAccess 3715
使用此政策 3715
政策詳細資訊 3715
政策版本 3716
JSON 政策文件 3716
進一步了解 3719
CloudWatchSyntheticsFullAccess 3719
使用此政策 3719
政策詳細資訊 3719
政策版本 3719
JSON 政策文件 3720
進一步了解 3725
CloudWatchSyntheticsReadOnlyAccess 3725
使用此政策 3725
政策詳細資訊 3725
政策版本 3725
JSON 政策文件 3725
進一步了解 3726
ComprehendDataAccessRolePolicy 3726
使用此政策 3726
政策詳細資訊 3726
政策版本 3727
JSON 政策文件 3727
進一步了解 3727
ComprehendFullAccess 3727
使用此政策 3728
政策詳細資訊 3728
政策版本 3728
JSON 政策文件 3728
進一步了解 3729
ComprehendMedicalFullAccess 3729
使用此政策 3729
政策詳細資訊 3729
政策版本 3729
JSON 政策文件 3729
進一步了解 3730

ComprehendReadOnly 3730
使用此政策 3730
政策詳細資訊 3730
政策版本 3730
JSON 政策文件 3731
進一步了解 3732
ComputeOptimizerAutomationServiceRolePolicy 3732
使用此政策 3732
政策詳細資訊 3732
政策版本 3733
JSON 政策文件 3733
進一步了解 3734
ComputeOptimizerReadOnlyAccess 3735
使用此政策 3735
政策詳細資訊 3735
政策版本 3735
JSON 政策文件 3735
進一步了解 3736
ComputeOptimizerServiceRolePolicy 3736
使用此政策 3737
政策詳細資訊 3737
政策版本 3737
JSON 政策文件 3737
進一步了解 3739
ConfigConformsServiceRolePolicy 3739
使用此政策 3739
政策詳細資訊 3739
政策版本 3739
JSON 政策文件 3739
進一步了解 3742
ConsoleFullAccessFromVercel 3742
使用此政策 3742
政策詳細資訊 3743
政策版本 3743
JSON 政策文件 3743
進一步了解 3747

ConsoleViewOnlyAccessFromVercel 3747
使用此政策 3747
政策詳細資訊 3747
政策版本 3747
JSON 政策文件 3747
進一步了解 3749
CostOptimizationHubAdminAccess 3750
使用此政策 3750
政策詳細資訊 3750
政策版本 3750
JSON 政策文件 3750
進一步了解 3751
CostOptimizationHubReadOnlyAccess 3752
使用此政策 3752
政策詳細資訊 3752
政策版本 3752
JSON 政策文件 3752
進一步了解 3753
CostOptimizationHubServiceRolePolicy 3753
使用此政策 3753
政策詳細資訊 3753
政策版本 3753
JSON 政策文件 3754
進一步了解 3755
CustomerProfilesServiceLinkedRolePolicy 3755
使用此政策 3755
政策詳細資訊 3755
政策版本 3755
JSON 政策文件 3756
進一步了解 3757
DatabaseAdministrator 3757
使用此政策 3757
政策詳細資訊 3757
政策版本 3757
JSON 政策文件 3758
進一步了解 3760

DataScientist 3760
使用此政策 3761
政策詳細資訊 3761
政策版本 3761
JSON 政策文件 3761
進一步了解 3765
DAXServiceRolePolicy 3765
使用此政策 3765
政策詳細資訊 3765
政策版本 3765
JSON 政策文件 3766
進一步了解 3766
DeclarativePoliciesEC2Report 3766
使用此政策 3766
政策詳細資訊 3767
政策版本 3767
JSON 政策文件 3767
進一步了解 3768
DynamoDBCloudWatchContributorInsightsServiceRolePolicy 3768
使用此政策 3768
政策詳細資訊 3768
政策版本 3768
JSON 政策文件 3768
進一步了解 3769
DynamoDBGlobalTableSettingsManagementServiceRolePolicy 3769
使用此政策 3769
政策詳細資訊 3769
政策版本 3770
JSON 政策文件 3770
進一步了解 3771
DynamoDBKinesisReplicationServiceRolePolicy 3771
使用此政策 3771
政策詳細資訊 3771
政策版本 3771
JSON 政策文件 3772
進一步了解 3772

DynamoDBReplicationServiceRolePolicy 3772
使用此政策 3773
政策詳細資訊 3773
政策版本 3773
JSON 政策文件 3773
進一步了解 3774
EC2FastLaunchFullAccess 3774
使用此政策 3775
政策詳細資訊 3775
政策版本 3775
JSON 政策文件 3775
進一步了解 3782
EC2FastLaunchServiceRolePolicy 3782
使用此政策 3782
政策詳細資訊 3782
政策版本 3783
JSON 政策文件 3783
進一步了解 3789
EC2FleetTimeShiftableServiceRolePolicy 3789
使用此政策 3789
政策詳細資訊 3789
政策版本 3789
JSON 政策文件 3790
進一步了解 3791
Ec2ImageBuilderCrossAccountDistributionAccess 3791
使用此政策 3791
政策詳細資訊 3791
政策版本 3792
JSON 政策文件 3792
進一步了解 3792
EC2ImageBuilderLifecycleExecutionPolicy 3793
使用此政策 3793
政策詳細資訊 3793
政策版本 3793
JSON 政策文件 3793
進一步了解 3795

EC2InstanceConnect 3795
使用此政策 3796
政策詳細資訊 3796
政策版本 3796
JSON 政策文件 3796
進一步了解 3796
Ec2InstanceConnectEndpoint 3797
使用此政策 3797
政策詳細資訊 3797
政策版本 3797
JSON 政策文件 3797
進一步了解 3800
EC2InstanceProfileForImageBuilder 3800
使用此政策 3800
政策詳細資訊 3800
政策版本 3800
JSON 政策文件 3801
進一步了解 3803
EC2InstanceProfileForImageBuilderECRContainerBuilds 3804
使用此政策 3804
政策詳細資訊 3804
政策版本 3804
JSON 政策文件 3804
進一步了解 3806
ECRReplicationServiceRolePolicy 3806
使用此政策 3806
政策詳細資訊 3806
政策版本 3806
JSON 政策文件 3806
進一步了解 3807
ECRTemplateServiceRolePolicy 3807
使用此政策 3807
政策詳細資訊 3807
政策版本 3807
JSON 政策文件 3808
進一步了解 3808

ElastiCacheServiceRolePolicy 3808
使用此政策 3808
政策詳細資訊 3808
政策版本 3809
JSON 政策文件 3809
進一步了解 3811
ElasticLoadBalancingFullAccess 3811
使用此政策 3811
政策詳細資訊 3811
政策版本 3811
JSON 政策文件 3812
進一步了解 3813
ElasticLoadBalancingReadOnly 3813
使用此政策 3813
政策詳細資訊 3813
政策版本 3814
JSON 政策文件 3814
進一步了解 3815
ElementalActivationsDownloadSoftwareAccess 3815
使用此政策 3815
政策詳細資訊 3815
政策版本 3815
JSON 政策文件 3816
進一步了解 3816
ElementalActivationsFullAccess 3816
使用此政策 3816
政策詳細資訊 3816
政策版本 3817
JSON 政策文件 3817
進一步了解 3817
ElementalActivationsGenerateLicenses 3817
使用此政策 3818
政策詳細資訊 3818
政策版本 3818
JSON 政策文件 3818
進一步了解 3818

ElementalActivationsReadOnlyAccess 3819
使用此政策 3819
政策詳細資訊 3819
政策版本 3819
JSON 政策文件 3819
進一步了解 3820
ElementalAppliancesSoftwareFullAccess 3820
使用此政策 3820
政策詳細資訊 3820
政策版本 3820
JSON 政策文件 3821
進一步了解 3821
ElementalAppliancesSoftwareReadOnlyAccess 3821
使用此政策 3821
政策詳細資訊 3821
政策版本 3822
JSON 政策文件 3822
進一步了解 3822
ElementalSupportCenterFullAccess 3822
使用此政策 3823
政策詳細資訊 3823
政策版本 3823
JSON 政策文件 3823
進一步了解 3823
EMRDescribeClusterPolicyForEMRWAL 3824
使用此政策 3824
政策詳細資訊 3824
政策版本 3824
JSON 政策文件 3824
進一步了解 3825
FMSServiceRolePolicy 3825
使用此政策 3825
政策詳細資訊 3825
政策版本 3825
JSON 政策文件 3826
進一步了解 3842

FSxDeleteServiceLinkedRoleAccess 3842
使用此政策 3842
政策詳細資訊 3842
政策版本 3843
JSON 政策文件 3843
進一步了解 3843
GameLiftContainerFleetPolicy 3843
使用此政策 3843
政策詳細資訊 3844
政策版本 3844
JSON 政策文件 3844
進一步了解 3845
GameLiftGameServerGroupPolicy 3845
使用此政策 3845
政策詳細資訊 3846
政策版本 3846
JSON 政策文件 3846
進一步了解 3847
GitLabDuoWithAmazonQPermissionsPolicy 3848
使用此政策 3848
政策詳細資訊 3848
政策版本 3848
JSON 政策文件 3848
進一步了解 3849
GlobalAcceleratorFullAccess 3849
使用此政策 3850
政策詳細資訊 3850
政策版本 3850
JSON 政策文件 3850
進一步了解 3851
GlobalAcceleratorReadOnlyAccess 3851
使用此政策 3851
政策詳細資訊 3852
政策版本 3852
JSON 政策文件 3852
進一步了解 3852

GreengrassOTAUpdateArtifactAccess 3853
使用此政策 3853
政策詳細資訊 3853
政策版本 3853
JSON 政策文件 3853
進一步了解 3854
GroundTruthSyntheticConsoleFullAccess 3854
使用此政策 3854
政策詳細資訊 3854
政策版本 3854
JSON 政策文件 3855
進一步了解 3855
GroundTruthSyntheticConsoleReadOnlyAccess 3855
使用此政策 3855
政策詳細資訊 3855
政策版本 3856
JSON 政策文件 3856
進一步了解 3856
Health_OrganizationsServiceRolePolicy 3856
使用此政策 3857
政策詳細資訊 3857
政策版本 3857
JSON 政策文件 3857
進一步了解 3858
IAMAccessAdvisorReadOnly 3858
使用此政策 3858
政策詳細資訊 3858
政策版本 3858
JSON 政策文件 3858
進一步了解 3859
IAMAccessAnalyzerFullAccess 3859
使用此政策 3860
政策詳細資訊 3860
政策版本 3860
JSON 政策文件 3860
進一步了解 3861

IAMAccessAnalyzerReadOnlyAccess 3861
使用此政策 3861
政策詳細資訊 3861
政策版本 3862
JSON 政策文件 3862
進一步了解 3862
IAMFullAccess 3863
使用此政策 3863
政策詳細資訊 3863
政策版本 3863
JSON 政策文件 3863
進一步了解 3864
IAMReadOnlyAccess 3864
使用此政策 3864
政策詳細資訊 3864
政策版本 3864
JSON 政策文件 3865
進一步了解 3865
IAMSelfManageServiceSpecificCredentials 3865
使用此政策 3865
政策詳細資訊 3866
政策版本 3866
JSON 政策文件 3866
進一步了解 3866
IAMUserChangePassword 3867
使用此政策 3867
政策詳細資訊 3867
政策版本 3867
JSON 政策文件 3867
進一步了解 3868
IAMUserSSHKeys 3868
使用此政策 3868
政策詳細資訊 3868
政策版本 3869
JSON 政策文件 3869
進一步了解 3869

IVSFullAccess 3869
使用此政策 3870
政策詳細資訊 3870
政策版本 3870
JSON 政策文件 3870
進一步了解 3870
IVSReadOnlyAccess 3871
使用此政策 3871
政策詳細資訊 3871
政策版本 3871
JSON 政策文件 3871
進一步了解 3872
IVSRecordToS3 3873
使用此政策 3873
政策詳細資訊 3873
政策版本 3873
JSON 政策文件 3873
進一步了解 3874
KafkaConnectServiceRolePolicy 3874
使用此政策 3874
政策詳細資訊 3874
政策版本 3874
JSON 政策文件 3875
進一步了解 3876
KafkaServiceRolePolicy 3876
使用此政策 3876
政策詳細資訊 3876
政策版本 3877
JSON 政策文件 3877
進一步了解 3879
KeyspacesCDCServiceRolePolicy 3879
使用此政策 3879
政策詳細資訊 3879
政策版本 3879
JSON 政策文件 3879
進一步了解 3880

KeyspacesReplicationServiceRolePolicy 3880
使用此政策 3880
政策詳細資訊 3880
政策版本 3880
JSON 政策文件 3881
進一步了解 3882
LakeFormationDataAccessServiceRolePolicy 3882
使用此政策 3882
政策詳細資訊 3882
政策版本 3883
JSON 政策文件 3883
進一步了解 3883
LexBotPolicy 3883
使用此政策 3884
政策詳細資訊 3884
政策版本 3884
JSON 政策文件 3884
進一步了解 3885
LexChannelPolicy 3885
使用此政策 3885
政策詳細資訊 3885
政策版本 3885
JSON 政策文件 3885
進一步了解 3886
LightsailExportAccess 3886
使用此政策 3886
政策詳細資訊 3886
政策版本 3886
JSON 政策文件 3887
進一步了解 3887
MediaConnectGatewayInstanceRolePolicy 3888
使用此政策 3888
政策詳細資訊 3888
政策版本 3888
JSON 政策文件 3888
進一步了解 3889

MediaPackageServiceRolePolicy 3889
使用此政策 3889
政策詳細資訊 3889
政策版本 3889
JSON 政策文件 3890
進一步了解 3890
MemoryDBServiceRolePolicy 3890
使用此政策 3890
政策詳細資訊 3890
政策版本 3891
JSON 政策文件 3891
進一步了解 3893
MigrationHubDMSAccessServiceRolePolicy 3893
使用此政策 3893
政策詳細資訊 3893
政策版本 3894
JSON 政策文件 3894
進一步了解 3895
MigrationHubServiceRolePolicy 3895
使用此政策 3895
政策詳細資訊 3895
政策版本 3895
JSON 政策文件 3896
進一步了解 3897
MigrationHubSMSAccessServiceRolePolicy 3897
使用此政策 3897
政策詳細資訊 3897
政策版本 3897
JSON 政策文件 3898
進一步了解 3899
MonitronServiceRolePolicy 3899
使用此政策 3899
政策詳細資訊 3899
政策版本 3899
JSON 政策文件 3899
進一步了解 3900

MultiPartyApprovalFullAccess 3900
使用此政策 3900
政策詳細資訊 3900
政策版本 3900
JSON 政策文件 3901
進一步了解 3903
MultiPartyApprovalReadOnlyAccess 3903
使用此政策 3903
政策詳細資訊 3903
政策版本 3904
JSON 政策文件 3904
進一步了解 3905
NeptuneConsoleFullAccess 3906
使用此政策 3906
政策詳細資訊 3906
政策版本 3906
JSON 政策文件 3906
進一步了解 3912
NeptuneFullAccess 3912
使用此政策 3912
政策詳細資訊 3912
政策版本 3913
JSON 政策文件 3913
進一步了解 3917
NeptuneGraphReadOnlyAccess 3917
使用此政策 3917
政策詳細資訊 3917
政策版本 3917
JSON 政策文件 3917
進一步了解 3919
NeptuneReadOnlyAccess 3919
使用此政策 3919
政策詳細資訊 3919
政策版本 3919
JSON 政策文件 3920
進一步了解 3922

NetworkAdministrator 3922
使用此政策 3922
政策詳細資訊 3922
政策版本 3922
JSON 政策文件 3923
進一步了解 3930
NetworkSecurityDirectorServiceLinkedRolePolicy 3930
使用此政策 3930
政策詳細資訊 3930
政策版本 3930
JSON 政策文件 3930
進一步了解 3936
NovaActServiceRolePolicy 3936
使用此政策 3936
政策詳細資訊 3936
政策版本 3936
JSON 政策文件 3936
進一步了解 3937
OAMFullAccess 3937
使用此政策 3937
政策詳細資訊 3937
政策版本 3937
JSON 政策文件 3938
進一步了解 3938
OAMReadOnlyAccess 3938
使用此政策 3938
政策詳細資訊 3938
政策版本 3939
JSON 政策文件 3939
進一步了解 3939
OpensearchIngestionSelfManagedVpcePolicy 3939
使用此政策 3939
政策詳細資訊 3940
政策版本 3940
JSON 政策文件 3940
進一步了解 3941

PartnerCentralAccountManagementUserRoleAssociation 3941
使用此政策 3941
政策詳細資訊 3941
政策版本 3941
JSON 政策文件 3941
進一步了解 3942
PartnerCentralIncentiveBenefitManagement 3942
使用此政策 3943
政策詳細資訊 3943
政策版本 3943
JSON 政策文件 3943
進一步了解 3947
PowerUserAccess 3947
使用此政策 3947
政策詳細資訊 3947
政策版本 3947
JSON 政策文件 3948
進一步了解 3948
QAppsServiceRolePolicy 3949
使用此政策 3949
政策詳細資訊 3949
政策版本 3949
JSON 政策文件 3949
進一步了解 3950
QBusinessQuicksightPluginPolicy 3950
使用此政策 3950
政策詳細資訊 3950
政策版本 3950
JSON 政策文件 3950
進一步了解 3951
QBusinessServiceRolePolicy 3951
使用此政策 3951
政策詳細資訊 3951
政策版本 3952
JSON 政策文件 3952
進一步了解 3953

QuickSightAccessForS3StorageManagementAnalyticsReadOnly 3953
使用此政策 3954
政策詳細資訊 3954
政策版本 3954
JSON 政策文件 3954
進一步了解 3955
RDSCloudHsmAuthorizationRole 3955
使用此政策 3955
政策詳細資訊 3955
政策版本 3955
JSON 政策文件 3956
進一步了解 3956
ReadOnlyAccess 3956
使用此政策 3956
政策詳細資訊 3957
政策版本 3957
JSON 政策文件 3957
進一步了解 4018
ResourceGroupsandTagEditorFullAccess 4019
使用此政策 4019
政策詳細資訊 4019
政策版本 4019
JSON 政策文件 4019
進一步了解 4020
ResourceGroupsandTagEditorReadOnlyAccess 4020
使用此政策 4020
政策詳細資訊 4020
政策版本 4020
JSON 政策文件 4021
進一步了解 4021
ResourceGroupsServiceRolePolicy 4021
使用此政策 4021
政策詳細資訊 4022
政策版本 4022
JSON 政策文件 4022
進一步了解 4022

ResourceGroupsTaggingAPITagUntagSupportedResources 4023
使用此政策 4023
政策詳細資訊 4023
政策版本 4023
JSON 政策文件 4023
進一步了解 4031
ROSAAmazonEBSCSIDriverOperatorPolicy 4032
使用此政策 4032
政策詳細資訊 4032
政策版本 4032
JSON 政策文件 4032
進一步了解 4035
ROSACloudNetworkConfigOperatorPolicy 4036
使用此政策 4036
政策詳細資訊 4036
政策版本 4036
JSON 政策文件 4036
進一步了解 4037
ROSAControlPlaneOperatorPolicy 4038
使用此政策 4038
政策詳細資訊 4038
政策版本 4038
JSON 政策文件 4038
進一步了解 4043
ROSAImageRegistryOperatorPolicy 4043
使用此政策 4043
政策詳細資訊 4043
政策版本 4043
JSON 政策文件 4043
進一步了解 4045
ROSAIngressOperatorPolicy 4045
使用此政策 4045
政策詳細資訊 4045
政策版本 4045
JSON 政策文件 4046
進一步了解 4046

ROSAInstallerPolicy 4047
使用此政策 4047
政策詳細資訊 4047
政策版本 4047
JSON 政策文件 4047
進一步了解 4056
ROSAKMSProviderPolicy 4056
使用此政策 4056
政策詳細資訊 4056
政策版本 4056
JSON 政策文件 4056
進一步了解 4057
ROSAKubeControllerPolicy 4057
使用此政策 4057
政策詳細資訊 4058
政策版本 4058
JSON 政策文件 4058
進一步了解 4062
ROSAManageSubscription 4062
使用此政策 4063
政策詳細資訊 4063
政策版本 4063
JSON 政策文件 4063
進一步了解 4064
ROSANodePoolManagementPolicy 4064
使用此政策 4064
政策詳細資訊 4064
政策版本 4065
JSON 政策文件 4065
進一步了解 4071
ROSASharedVPCEndpointPolicy 4071
使用此政策 4071
政策詳細資訊 4071
政策版本 4071
JSON 政策文件 4072
進一步了解 4075

ROSASharedVPCRoute53Policy 4076
使用此政策 4076
政策詳細資訊 4076
政策版本 4076
JSON 政策文件 4076
進一步了解 4077
ROSASRESupportPolicy 4078
使用此政策 4078
政策詳細資訊 4078
政策版本 4078
JSON 政策文件 4078
進一步了解 4083
ROSAWorkerInstancePolicy 4083
使用此政策 4083
政策詳細資訊 4083
政策版本 4084
JSON 政策文件 4084
進一步了解 4085
Route53RecoveryReadinessServiceRolePolicy 4085
使用此政策 4085
政策詳細資訊 4085
政策版本 4086
JSON 政策文件 4086
進一步了解 4089
Route53ResolverServiceRolePolicy 4089
使用此政策 4089
政策詳細資訊 4090
政策版本 4090
JSON 政策文件 4090
進一步了解 4090
RTBFabricServiceRolePolicy 4091
使用此政策 4091
政策詳細資訊 4091
政策版本 4091
JSON 政策文件 4091
進一步了解 4093

S3StorageLensServiceRolePolicy 4094
使用此政策 4094
政策詳細資訊 4094
政策版本 4094
JSON 政策文件 4094
進一步了解 4095
SageMakerStudioAdminIAMConsolePolicy 4095
使用此政策 4095
政策詳細資訊 4095
政策版本 4095
JSON 政策文件 4096
進一步了解 4106
SageMakerStudioAdminIAMDefaultExecutionPolicy 4107
使用此政策 4107
政策詳細資訊 4107
政策版本 4107
JSON 政策文件 4107
進一步了解 4128
SageMakerStudioAdminIAMPermissiveExecutionPolicy 4129
使用此政策 4129
政策詳細資訊 4129
政策版本 4129
JSON 政策文件 4129
進一步了解 4145
SageMakerStudioAdminProjectUserRolePolicy 4145
使用此政策 4145
政策詳細資訊 4146
政策版本 4146
JSON 政策文件 4146
進一步了解 4148
SageMakerStudioBedrockAgentServiceRolePolicy 4149
使用此政策 4149
政策詳細資訊 4149
政策版本 4149
JSON 政策文件 4149
進一步了解 4153

SageMakerStudioBedrockChatAgentUserRolePolicy 4153
使用此政策 4153
政策詳細資訊 4153
政策版本 4153
JSON 政策文件 4153
進一步了解 4158
SageMakerStudioBedrockEvaluationJobServiceRolePolicy 4158
使用此政策 4158
政策詳細資訊 4158
政策版本 4158
JSON 政策文件 4158
進一步了解 4162
SageMakerStudioBedrockFlowServiceRolePolicy 4162
使用此政策 4162
政策詳細資訊 4162
政策版本 4163
JSON 政策文件 4163
進一步了解 4167
SageMakerStudioBedrockFunctionExecutionRolePolicy 4167
使用此政策 4167
政策詳細資訊 4167
政策版本 4167
JSON 政策文件 4167
進一步了解 4168
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 4169
使用此政策 4169
政策詳細資訊 4169
政策版本 4169
JSON 政策文件 4169
進一步了解 4170
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy 4170
使用此政策 4171
政策詳細資訊 4171
政策版本 4171
JSON 政策文件 4171
進一步了解 4177

SageMakerStudioBedrockPromptUserRolePolicy 4177
使用此政策 4177
政策詳細資訊 4177
政策版本 4177
JSON 政策文件 4177
進一步了解 4180
SageMakerStudioDomainExecutionRolePolicy 4180
使用此政策 4180
政策詳細資訊 4180
政策版本 4180
JSON 政策文件 4181
進一步了解 4187
SageMakerStudioDomainServiceRolePolicy 4187
使用此政策 4187
政策詳細資訊 4187
政策版本 4188
JSON 政策文件 4188
進一步了解 4189
SageMakerStudioEMRContainersSystemNamespaceRolePolicy 4189
使用此政策 4189
政策詳細資訊 4189
政策版本 4189
JSON 政策文件 4190
進一步了解 4191
SageMakerStudioEMRInstanceRolePolicy 4191
使用此政策 4192
政策詳細資訊 4192
政策版本 4192
JSON 政策文件 4192
進一步了解 4195
SageMakerStudioEMRServiceRolePolicy 4196
使用此政策 4196
政策詳細資訊 4196
政策版本 4196
JSON 政策文件 4196
進一步了解 4198

SageMakerStudioFullAccess 4199
使用此政策 4199
政策詳細資訊 4199
政策版本 4199
JSON 政策文件 4199
進一步了解 4209
SageMakerStudioProjectProvisioningRolePolicy 4210
使用此政策 4210
政策詳細資訊 4210
政策版本 4210
JSON 政策文件 4210
進一步了解 4279
SageMakerStudioProjectRoleMachineLearningPolicy 4279
使用此政策 4279
政策詳細資訊 4280
政策版本 4280
JSON 政策文件 4280
進一步了解 4309
SageMakerStudioProjectUserRolePermissionsBoundary 4310
使用此政策 4310
政策詳細資訊 4310
政策版本 4310
JSON 政策文件 4310
進一步了解 4365
SageMakerStudioProjectUserRolePolicy 4366
使用此政策 4366
政策詳細資訊 4366
政策版本 4366
JSON 政策文件 4366
進一步了解 4432
SageMakerStudioQueryExecutionRolePolicy 4432
使用此政策 4432
政策詳細資訊 4432
政策版本 4432
JSON 政策文件 4432
進一步了解 4434

SageMakerStudioUserIAMConsolePolicy 4434
使用此政策 4435
政策詳細資訊 4435
政策版本 4435
JSON 政策文件 4435
進一步了解 4437
SageMakerStudioUserIAMDefaultExecutionPolicy 4437
使用此政策 4437
政策詳細資訊 4437
政策版本 4437
JSON 政策文件 4437
進一步了解 4459
SageMakerStudioUserIAMPermissiveExecutionPolicy 4459
使用此政策 4460
政策詳細資訊 4460
政策版本 4460
JSON 政策文件 4460
進一步了解 4474
SecretsManagerReadWrite 4475
使用此政策 4475
政策詳細資訊 4475
政策版本 4475
JSON 政策文件 4475
進一步了解 4477
SecurityAgentWebAppAPIPolicy 4477
使用此政策 4477
政策詳細資訊 4477
政策版本 4477
JSON 政策文件 4478
進一步了解 4479
SecurityAgentWebAppPolicy 4479
使用此政策 4480
政策詳細資訊 4480
政策版本 4480
JSON 政策文件 4480
進一步了解 4482

SecurityAudit 4482
使用此政策 4482
政策詳細資訊 4482
政策版本 4482
JSON 政策文件 4482
進一步了解 4504
SecurityLakeResourceManagementServiceRolePolicy 4505
使用此政策 4505
政策詳細資訊 4505
政策版本 4505
JSON 政策文件 4505
進一步了解 4511
SecurityLakeServiceLinkedRole 4511
使用此政策 4511
政策詳細資訊 4511
政策版本 4511
JSON 政策文件 4512
進一步了解 4514
ServerMigration_ServiceRole 4515
使用此政策 4515
政策詳細資訊 4515
政策版本 4515
JSON 政策文件 4515
進一步了解 4520
ServerMigrationConnector 4520
使用此政策 4520
政策詳細資訊 4520
政策版本 4521
JSON 政策文件 4521
進一步了解 4522
ServerMigrationServiceConsoleFullAccess 4523
使用此政策 4523
政策詳細資訊 4523
政策版本 4523
JSON 政策文件 4523
進一步了解 4525

ServerMigrationServiceLaunchRole 4525
使用此政策 4525
政策詳細資訊 4525
政策版本 4525
JSON 政策文件 4526
進一步了解 4528
ServerMigrationServiceRoleForInstanceValidation 4529
使用此政策 4529
政策詳細資訊 4529
政策版本 4529
JSON 政策文件 4529
進一步了解 4530
ServiceQuotasFullAccess 4530
使用此政策 4530
政策詳細資訊 4530
政策版本 4530
JSON 政策文件 4531
進一步了解 4532
ServiceQuotasReadOnlyAccess 4532
使用此政策 4533
政策詳細資訊 4533
政策版本 4533
JSON 政策文件 4533
進一步了解 4534
ServiceQuotasServiceRolePolicy 4535
使用此政策 4535
政策詳細資訊 4535
政策版本 4535
JSON 政策文件 4535
進一步了解 4536
SignInLocalDevelopmentAccess 4536
使用此政策 4536
政策詳細資訊 4536
政策版本 4536
JSON 政策文件 4536
進一步了解 4537

SimpleWorkflowFullAccess 4537
使用此政策 4537
政策詳細資訊 4537
政策版本 4537
JSON 政策文件 4538
進一步了解 4538
SMSVoiceServiceRolePolicy 4538
使用此政策 4538
政策詳細資訊 4538
政策版本 4539
JSON 政策文件 4539
進一步了解 4539
SplitCostAllocationDataServiceRolePolicy 4539
使用此政策 4540
政策詳細資訊 4540
政策版本 4540
JSON 政策文件 4540
進一步了解 4541
SSMQuickSetupRolePolicy 4541
使用此政策 4541
政策詳細資訊 4541
政策版本 4541
JSON 政策文件 4542
進一步了解 4544
SupportUser 4545
使用此政策 4545
政策詳細資訊 4545
政策版本 4545
JSON 政策文件 4545
進一步了解 4550
SystemAdministrator 4551
使用此政策 4551
政策詳細資訊 4551
政策版本 4551
JSON 政策文件 4551
進一步了解 4557

TranslateFullAccess 4558
使用此政策 4558
政策詳細資訊 4558
政策版本 4558
JSON 政策文件 4558
進一步了解 4559
TranslateReadOnly 4559
使用此政策 4559
政策詳細資訊 4559
政策版本 4559
JSON 政策文件 4560
進一步了解 4560
ViewOnlyAccess 4560
使用此政策 4561
政策詳細資訊 4561
政策版本 4561
JSON 政策文件 4561
進一步了解 4570
VMImportExportRoleForAWSConnector 4571
使用此政策 4571
政策詳細資訊 4571
政策版本 4571
JSON 政策文件 4571
進一步了解 4572
VPCLatticeFullAccess 4572
使用此政策 4572
政策詳細資訊 4572
政策版本 4573
JSON 政策文件 4573
進一步了解 4575
VPCLatticeReadOnlyAccess 4575
使用此政策 4575
政策詳細資訊 4575
政策版本 4575
JSON 政策文件 4576
進一步了解 4576

VPCLatticeServicesInvokeAccess 4577
使用此政策 4577
政策詳細資訊 4577
政策版本 4577
JSON 政策文件 4577
進一步了解 4578
WAFLoggingServiceRolePolicy 4578
使用此政策 4578
政策詳細資訊 4578
政策版本 4578
JSON 政策文件 4579
進一步了解 4579
WAFRegionalLoggingServiceRolePolicy 4579
使用此政策 4579
政策詳細資訊 4579
政策版本 4580
JSON 政策文件 4580
進一步了解 4580
WAFV2LoggingServiceRolePolicy 4580
使用此政策 4581
政策詳細資訊 4581
政策版本 4581
JSON 政策文件 4581
進一步了解 4582
WellArchitectedConsoleFullAccess 4582
使用此政策 4582
政策詳細資訊 4582
政策版本 4582
JSON 政策文件 4582
進一步了解 4583
WellArchitectedConsoleReadOnlyAccess 4583
使用此政策 4583
政策詳細資訊 4583
政策版本 4583
JSON 政策文件 4584
進一步了解 4584

WorkLinkServiceRolePolicy 4584
使用此政策 4584
政策詳細資訊 4584
政策版本 4585
JSON 政策文件 4585
進一步了解 4585
..... mmmmdlxxxvii

什麼是 AWS 受管政策？

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策，旨在為許多常用案例提供許可。與必須自行撰寫政策相比，它們可讓您更輕鬆地開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為它們可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新 AWS 服務啟動或新 API 操作可用於現有服務時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

了解政策參考頁面

每個政策參考頁面都包含下列資訊：

- 使用此政策 – 是否可將政策連接至使用者、群組和角色
- 政策詳細資訊
  - 類型 – AWS 受管政策的類型
    - `AWS managed policy` – 標準 AWS 受管政策
    - `Job function policy` – 符合常見產業任務功能的政策
    - `Service-linked role policy` – 連接到服務連結角色的政策，允許服務代表您執行動作，例如 the section called “AmazonRDSPreviewServiceRolePolicy”
    - `Service role policy` – 旨在使用 服務角色的政策，例如 the section called “AWSControlTowerServiceRolePolicy”
  - 建立時間 – 第一次建立政策時
  - 編輯時間 – 編輯此版本政策時
  - ARN – 政策的 Amazon Resource Name
- 政策版本 – 政策授予的許可版本
- JSON 政策文件 – 政策 JSON
- 進一步了解 – 連結至與 AWS 受管政策相關的文件

已棄用 AWS 受管政策

AWS 會定期更新 AWS 受管政策。在大多數情況下，我們會將許可新增至政策。當我們啟動新的服務或功能時，就會發生這種情況。為了改善受管 AWS 政策的安全性，我們有時會減少政策的範圍。當我們從政策移除許可時，會將政策設定為已棄用狀態，並使新的狀態可用。當 棄 AWS 用服務或功能時，我們也棄用該功能的 AWS 受管政策。

如果您收到電子郵件通知，指出您使用的政策已遭取代，建議您立即採取動作。識別政策的變更並更新您的工作流程。如果 AWS 提供替代政策，請計劃將其連接到所有受影響的身分 （使用者、群組和角色），然後將已取代的政策從這些身分分離。

已作廢的政策具有以下特點：

- 它已從本指南中移除。
- 許可會繼續適用於所有目前連接的身分。
- 在政策連接到身分的帳戶中，它會出現在 IAM 主控台的政策清單中，旁邊有一個警告圖示。
- 它無法連接到任何新的身分。如果您將其與目前身分分離，則無法重新連接。
- 將其從所有目前實體分離後，就不會再顯示。

AWS 受管政策

AWS 受管政策

- AccessAnalyzerServiceRolePolicy
- AccountManagementFromVercel
- AdministratorAccess
- AdministratorAccess-Amplify
- AdministratorAccess-AWSElasticBeanstalk
- AIOpsAssistantIncidentReportPolicy
- AIOpsAssistantPolicy
- AIOpsConsoleAdminPolicy
- AIOpsOperatorAccess
- AIOpsReadOnlyAccess
- AlexaForBusinessDeviceSetup
- AlexaForBusinessFullAccess
- AlexaForBusinessGatewayExecution
- AlexaForBusinessLifesizeDelegatedAccessPolicy
- AlexaForBusinessNetworkProfileServicePolicy
- AlexaForBusinessPolyDelegatedAccessPolicy
- AlexaForBusinessReadOnlyAccess
- AmazonAPIGatewayAdministrator
- AmazonAPIGatewayInvokeFullAccess
- AmazonAPIGatewayPushToCloudWatchLogs
- AmazonAppFlowFullAccess
- AmazonAppFlowReadOnlyAccess
- AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy
- AmazonAppStreamFullAccess
- AmazonAppStreamPCAAccess
- AmazonAppStreamReadOnlyAccess

- AmazonAppStreamServiceAccess
- AmazonAthenaFullAccess
- AmazonAthenaServiceRolePolicy
- AmazonAugmentedAIFullAccess
- AmazonAugmentedAIHumanLoopFullAccess
- AmazonAugmentedAIIntegratedAPIAccess
- AmazonAuroraDSQLConsoleFullAccess
- AmazonAuroraDSQLFullAccess
- AmazonAuroraDSQLReadOnlyAccess
- AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy
- AmazonBedrockFullAccess
- AmazonBedrockLimitedAccess
- AmazonBedrockMantleFullAccess
- AmazonBedrockMantleInferenceAccess
- AmazonBedrockMantleReadOnly
- AmazonBedrockMarketplaceAccess
- AmazonBedrockReadOnly
- AmazonBedrockStudioPermissionsBoundary
- 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
- AmazonDataZoneBedrockModelConsumptionPolicy
- AmazonDataZoneBedrockModelManagementPolicy
- AmazonDataZoneDomainExecutionRolePolicy
- AmazonDataZoneEnvironmentRolePermissionsBoundary
- AmazonDataZoneFullAccess
- AmazonDataZoneFullUserAccess
- AmazonDataZoneGlueManageAccessRolePolicy
- AmazonDataZonePortalFullAccessPolicy
- AmazonDataZonePreviewConsoleFullAccess
- AmazonDataZoneProjectDeploymentPermissionsBoundary
- AmazonDataZoneProjectRolePermissionsBoundary
- AmazonDataZoneRedshiftGlueProvisioningPolicy
- AmazonDataZoneRedshiftManageAccessRolePolicy
- AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- AmazonDataZoneSageMakerManageAccessRolePolicy
- AmazonDataZoneSageMakerProvisioningRolePolicy
- AmazonDetectiveFullAccess
- AmazonDetectiveInvestigatorAccess
- AmazonDetectiveMemberAccess
- AmazonDetectiveOrganizationsAccess
- AmazonDetectiveServiceLinkedRolePolicy
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruOrganizationsAccess
- AmazonDevOpsGuruReadOnlyAccess

- AmazonDevOpsGuruServiceRolePolicy
- AmazonDMSCloudWatchLogsRole
- AmazonDMSRedshiftS3Role
- AmazonDMSVPCManagementRole
- AmazonDocDB-ElasticServiceRolePolicy
- AmazonDocDBConsoleFullAccess
- AmazonDocDBElasticFullAccess
- AmazonDocDBElasticReadOnlyAccess
- AmazonDocDBFullAccess
- AmazonDocDBReadOnlyAccess
- AmazonDRSVPCManagement
- AmazonDynamoDBFullAccess
- AmazonDynamoDBFullAccess_v2
- AmazonDynamoDBFullAccesswithDataPipeline
- AmazonDynamoDBReadOnlyAccess
- AmazonEBSCSIDriverPolicy
- AmazonEC2ContainerRegistryFullAccess
- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryPullOnly
- AmazonEC2ContainerRegistryReadOnly
- AmazonEC2ContainerServiceAutoscaleRole
- AmazonEC2ContainerServiceEventsRole
- AmazonEC2ContainerServiceforEC2Role
- AmazonEC2ContainerServiceRole
- AmazonEC2FullAccess
- AmazonEC2ImageReferencesAccessPolicy
- AmazonEC2ReadOnlyAccess
- AmazonEC2RoleforAWSCodeDeploy
- AmazonEC2RoleforAWSCodeDeployLimited

- AmazonEC2RoleforDataPipelineRole
- AmazonEC2RoleforSSM
- AmazonEC2RolePolicyForLaunchWizard
- AmazonEC2SpotFleetAutoscaleRole
- AmazonEC2SpotFleetTaggingRole
- AmazonECS_FullAccess
- AmazonECSComputeServiceRolePolicy
- AmazonECSInfrastructureRoleforExpressGatewayServices
- AmazonECSInfrastructureRolePolicyForLoadBalancers
- AmazonECSInfrastructureRolePolicyForManagedInstances
- AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
- AmazonECSInfrastructureRolePolicyForVolumes
- AmazonECSInfrastructureRolePolicyForVpcLattice
- AmazonECSInstanceRolePolicyForManagedInstances
- AmazonECSServiceRolePolicy
- AmazonECSTaskExecutionRolePolicy
- AmazonEFSCSIDriverPolicy
- AmazonEKS_CNI_Policy
- AmazonEKSBlockStoragePolicy
- AmazonEKSClusterPolicy
- AmazonEKSComputePolicy
- AmazonEKSConnectorServiceRolePolicy
- AmazonEKSDashboardConsoleReadOnly
- AmazonEKSDashboardServiceRolePolicy
- AmazonEKSFargatePodExecutionRolePolicy
- AmazonEKSForFargateServiceRolePolicy
- AmazonEKSLoadBalancingPolicy
- AmazonEKSLocalOutpostClusterPolicy
- AmazonEKSLocalOutpostServiceRolePolicy
- AmazonEKSMCPReadOnlyAccess

- AmazonEKSNetworkingPolicy
- AmazonEKSServicePolicy
- AmazonEKSServiceRolePolicy
- AmazonEKSVPCResourceController
- AmazonEKSWorkerNodeMinimalPolicy
- 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
- AmazonEVSServiceRolePolicy
- AmazonFISServiceRolePolicy
- AmazonForecastFullAccess
- AmazonFraudDetectorFullAccessPolicy
- AmazonFreeRTOSFullAccess
- AmazonFreeRTOSOTAUpdate
- AmazonFSxConsoleFullAccess
- AmazonFSxConsoleReadOnlyAccess
- AmazonFSxFullAccess
- AmazonFSxReadOnlyAccess

- AmazonFSxServiceRolePolicy
- AmazonGlacierFullAccess
- AmazonGlacierReadOnlyAccess
- AmazonGrafanaAthenaAccess
- AmazonGrafanaCloudWatchAccess
- AmazonGrafanaRedshiftAccess
- AmazonGrafanaServiceLinkedRolePolicy
- AmazonGuardDutyFullAccess
- AmazonGuardDutyFullAccess_v2
- AmazonGuardDutyMalwareProtectionServiceRolePolicy
- AmazonGuardDutyReadOnlyAccess
- AmazonGuardDutyServiceRolePolicy
- AmazonHealthLakeFullAccess
- AmazonHealthLakeReadOnlyAccess
- AmazonHoneycodeFullAccess
- AmazonHoneycodeReadOnlyAccess
- AmazonHoneycodeServiceRolePolicy
- AmazonHoneycodeTeamAssociationFullAccess
- AmazonHoneycodeTeamAssociationReadOnlyAccess
- AmazonHoneycodeWorkbookFullAccess
- AmazonHoneycodeWorkbookReadOnlyAccess
- AmazonInspector2AgentlessServiceRolePolicy
- AmazonInspector2FullAccess
- AmazonInspector2FullAccess_v2
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ManagedTelemetryPolicy
- 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
- AmazonMWAAServerlessServiceRolePolicy
- AmazonMWAAServiceRolePolicy
- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser
- AmazonODBServiceRolePolicy
- AmazonOmicsFullAccess
- AmazonOmicsReadOnlyAccess
- AmazonOneEnterpriseFullAccess
- AmazonOneEnterpriseInstallerAccess
- AmazonOneEnterpriseReadOnlyAccess
- AmazonOpenSearchDashboardsServiceRolePolicy
- AmazonOpenSearchDirectQueryGlueCreateAccess
- AmazonOpenSearchIngestionFullAccess
- AmazonOpenSearchIngestionReadOnlyAccess
- AmazonOpenSearchIngestionServiceRolePolicy
- AmazonOpenSearchServerlessServiceRolePolicy
- AmazonOpenSearchServiceCognitoAccess
- AmazonOpenSearchServiceFullAccess
- AmazonOpenSearchServiceReadOnlyAccess
- AmazonOpenSearchServiceRolePolicy
- AmazonPersonalizeFullAccess
- AmazonPollyFullAccess
- AmazonPollyReadOnlyAccess
- AmazonPrometheusConsoleFullAccess

- AmazonPrometheusFullAccess
- AmazonPrometheusQueryAccess
- AmazonPrometheusRemoteWriteAccess
- AmazonPrometheusScraperServiceRolePolicy
- AmazonQDeveloperAccess
- AmazonQFullAccess
- AmazonQLDBConsoleFullAccess
- AmazonQLDBFullAccess
- AmazonQLDBReadOnly
- AmazonRDSBetaServiceRolePolicy
- AmazonRDSCustomInstanceProfileRolePolicy
- AmazonRDSCustomPreviewServiceRolePolicy
- AmazonRDSCustomServiceRolePolicy
- AmazonRDSDataFullAccess
- AmazonRDSDirectoryServiceAccess
- AmazonRDSEnhancedMonitoringRole
- AmazonRDSFullAccess
- AmazonRDSPerformanceInsightsFullAccess
- AmazonRDSPerformanceInsightsReadOnly
- AmazonRDSPreviewServiceRolePolicy
- AmazonRDSReadOnlyAccess
- AmazonRDSServiceRolePolicy
- AmazonRedshiftAllCommandsFullAccess
- AmazonRedshiftDataFullAccess
- AmazonRedshiftFederatedAuthorization
- AmazonRedshiftFullAccess
- AmazonRedshiftQueryEditor
- AmazonRedshiftQueryEditorV2FullAccess
- AmazonRedshiftQueryEditorV2NoSharing
- AmazonRedshiftQueryEditorV2ReadSharing

- AmazonRedshiftQueryEditorV2ReadWriteSharing
- AmazonRedshiftReadOnlyAccess
- AmazonRedshiftServiceLinkedRolePolicy
- AmazonRekognitionCustomLabelsFullAccess
- AmazonRekognitionFullAccess
- AmazonRekognitionReadOnlyAccess
- AmazonRekognitionServiceRole
- AmazonRoute53AutoNamingFullAccess
- AmazonRoute53AutoNamingReadOnlyAccess
- AmazonRoute53AutoNamingRegistrantAccess
- AmazonRoute53DomainsFullAccess
- AmazonRoute53DomainsReadOnlyAccess
- AmazonRoute53FullAccess
- AmazonRoute53GlobalResolverFullAccess
- AmazonRoute53GlobalResolverReadOnlyAccess
- AmazonRoute53ProfilesFullAccess
- AmazonRoute53ProfilesReadOnlyAccess
- AmazonRoute53ReadOnlyAccess
- AmazonRoute53RecoveryClusterFullAccess
- AmazonRoute53RecoveryClusterReadOnlyAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryControlConfigReadOnlyAccess
- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53RecoveryReadinessReadOnlyAccess
- AmazonRoute53ResolverFullAccess
- AmazonRoute53ResolverReadOnlyAccess
- AmazonS3FullAccess
- AmazonS3ObjectLambdaExecutionRolePolicy
- AmazonS3OutpostsFullAccess
- AmazonS3OutpostsReadOnlyAccess

- AmazonS3ReadOnlyAccess
- AmazonS3TablesFullAccess
- AmazonS3TablesLakeFormationServiceRole
- AmazonS3TablesReadOnlyAccess
- AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy
- AmazonSageMakerCanvasAIServicesAccess
- AmazonSageMakerCanvasBedrockAccess
- AmazonSageMakerCanvasDataPrepFullAccess
- AmazonSageMakerCanvasDirectDeployAccess
- AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy
- AmazonSageMakerCanvasForecastAccess
- AmazonSageMakerCanvasFullAccess
- AmazonSageMakerCanvasSMDataScienceAssistantAccess
- AmazonSageMakerClusterInstanceRolePolicy
- AmazonSageMakerCoreServiceRolePolicy
- AmazonSageMakerEdgeDeviceFleetPolicy
- AmazonSageMakerFeatureStoreAccess
- AmazonSageMakerFullAccess
- AmazonSageMakerGeospatialExecutionRole
- AmazonSageMakerGeospatialFullAccess
- AmazonSageMakerGroundTruthExecution
- AmazonSageMakerHyperPodGatedModelAccess
- AmazonSageMakerHyperPodInferenceAccess
- AmazonSageMakerHyperPodObservabilityAdminAccess
- AmazonSageMakerHyperPodServiceRolePolicy
- AmazonSageMakerHyperPodTrainingOperatorAccess
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy

- AmazonSageMakerPartnerAppsFullAccess
- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerQuickSightVPCPolicy
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerSpacesControllerPolicy
- AmazonSageMakerSpacesRouterPolicy
- AmazonSageMakerTrainingPlanCreateAccess
- AmazonSecurityLakeAdministrator
- AmazonSecurityLakeMetastoreManager
- AmazonSecurityLakePermissionsBoundary
- AmazonSESFullAccess
- AmazonSESReadOnlyAccess
- AmazonSESServiceRolePolicy
- AmazonSNSFullAccess
- AmazonSNSReadOnlyAccess
- AmazonSNSRole
- AmazonSQSFullAccess
- AmazonSQSReadOnlyAccess
- AmazonSSMAutomationApproverAccess

- AmazonSSMAutomationRole
- AmazonSSMDirectoryServiceAccess
- AmazonSSMFullAccess
- AmazonSSMMaintenanceWindowRole
- AmazonSSMManagedEC2InstanceDefaultPolicy
- AmazonSSMManagedInstanceCore
- AmazonSSMPatchAssociation
- AmazonSSMReadOnlyAccess
- AmazonSSMServiceRolePolicy
- AmazonSumerianFullAccess
- AmazonTextractFullAccess
- AmazonTextractServiceRole
- AmazonTimestreamConsoleFullAccess
- AmazonTimestreamFullAccess
- AmazonTimestreamInfluxDBFullAccess
- AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess
- AmazonTimestreamInfluxDBServiceRolePolicy
- AmazonTimestreamReadOnlyAccess
- AmazonTranscribeFullAccess
- AmazonTranscribeReadOnlyAccess
- AmazonVerifiedPermissionsFullAccess
- AmazonVerifiedPermissionsReadOnlyAccess
- AmazonVPCCrossAccountNetworkInterfaceOperations
- AmazonVPCFullAccess
- AmazonVPCNetworkAccessAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
- AmazonVPCReadOnlyAccess
- AmazonWorkDocsFullAccess
- AmazonWorkDocsReadOnlyAccess

- AmazonWorkMailEventsServiceRolePolicy
- AmazonWorkMailFullAccess
- AmazonWorkMailMessageFlowFullAccess
- AmazonWorkMailMessageFlowReadOnlyAccess
- AmazonWorkMailReadOnlyAccess
- AmazonWorkSpacesAdmin
- AmazonWorkSpacesApplicationManagerAdminAccess
- AmazonWorkspacesPCAAccess
- AmazonWorkSpacesPoolServiceAccess
- AmazonWorkSpacesSecureBrowserReadOnly
- AmazonWorkSpacesSelfServiceAccess
- AmazonWorkSpacesServiceAccess
- AmazonWorkSpacesThinClientFullAccess
- AmazonWorkSpacesThinClientMonitoringServiceRolePolicy
- AmazonWorkSpacesThinClientReadOnlyAccess
- AmazonWorkSpacesWebReadOnly
- AmazonWorkSpacesWebServiceRolePolicy
- AmazonZocaloFullAccess
- AmazonZocaloReadOnlyAccess
- AmplifyBackendDeployFullAccess
- APIGatewayServiceRolePolicy
- AppIntegrationsServiceLinkedRolePolicy
- ApplicationAutoScalingForAmazonAppStreamAccess
- ApplicationDiscoveryServiceContinuousExportServiceRolePolicy
- AppRunnerNetworkingServiceRolePolicy
- AppRunnerServiceRolePolicy
- AppStudioServiceRolePolicy
- AuroraDsqlServiceLinkedRolePolicy
- AutoScalingConsoleFullAccess
- AutoScalingConsoleReadOnlyAccess

- AutoScalingFullAccess
- AutoScalingNotificationAccessRole
- AutoScalingReadOnlyAccess
- AutoScalingServiceRolePolicy
- AWS-SSM-Automation-DiagnosisBucketPolicy
- AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy
- AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy
- AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy
- AWS-SSM-RemediationAutomation-AdministrationRolePolicy
- AWS-SSM-RemediationAutomation-ExecutionRolePolicy
- AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy
- AWS_ConfigRole
- AWSAccountActivityAccess
- AWSAccountManagementFullAccess
- AWSAccountManagementReadOnlyAccess
- AWSAccountSettingsManagementRole
- AWSAccountUsageReportAccess
- AWSAgentlessDiscoveryService
- AWSAppFabricFullAccess
- AWSAppFabricReadOnlyAccess
- AWSAppFabricServiceRolePolicy
- AWSApplicationAutoscalingAppStreamFleetPolicy
- AWSApplicationAutoscalingCassandraTablePolicy
- AWSApplicationAutoscalingComprehendEndpointPolicy
- AWSApplicationAutoScalingCustomResourcePolicy
- AWSApplicationAutoscalingDynamoDBTablePolicy
- AWSApplicationAutoscalingEC2SpotFleetRequestPolicy
- AWSApplicationAutoscalingECSServicePolicy
- AWSApplicationAutoscalingElastiCacheRGPolicy
- AWSApplicationAutoscalingEMRInstanceGroupPolicy

- AWSApplicationAutoscalingKafkaClusterPolicy
- AWSApplicationAutoscalingLambdaConcurrencyPolicy
- AWSApplicationAutoscalingNeptuneClusterPolicy
- AWSApplicationAutoscalingRDSClusterPolicy
- AWSApplicationAutoscalingSageMakerEndpointPolicy
- AWSApplicationAutoscalingWorkSpacesPoolPolicy
- AWSApplicationDiscoveryAgentAccess
- AWSApplicationDiscoveryAgentlessCollectorAccess
- AWSApplicationDiscoveryServiceFullAccess
- AWSApplicationMigrationAgentInstallationPolicy
- AWSApplicationMigrationAgentPolicy
- AWSApplicationMigrationAgentPolicy_v2
- AWSApplicationMigrationConversionServerPolicy
- AWSApplicationMigrationEC2Access
- AWSApplicationMigrationFullAccess
- AWSApplicationMigrationMGHAccess
- AWSApplicationMigrationNetworkMigrationCustomResource
- AWSApplicationMigrationNetworkMigrationMultiAccount
- AWSApplicationMigrationReadOnlyAccess
- AWSApplicationMigrationReplicationServerPolicy
- AWSApplicationMigrationServiceEc2InstancePolicy
- AWSApplicationMigrationServiceRolePolicy
- AWSApplicationMigrationSSMAccess
- AWSApplicationMigrationVCenterClientPolicy
- AWSAppMeshEnvoyAccess
- AWSAppMeshFullAccess
- AWSAppMeshPreviewEnvoyAccess
- AWSAppMeshPreviewServiceRolePolicy
- AWSAppMeshReadOnly
- AWSAppMeshServiceRolePolicy

- AWSAppRunnerFullAccess
- AWSAppRunnerReadOnlyAccess
- AWSAppRunnerServicePolicyForECRAccess
- AWSAppSyncAdministrator
- AWSAppSyncInvokeFullAccess
- AWSAppSyncPushToCloudWatchLogs
- AWSAppSyncSchemaAuthor
- AWSAppSyncServiceRolePolicy
- AWSArtifactAccountSync
- AWSArtifactAgreementsFullAccess
- AWSArtifactAgreementsReadOnlyAccess
- AWSArtifactReportsReadOnlyAccess
- AWSArtifactServiceRolePolicy
- AWSAuditManagerAdministratorAccess
- AWSAuditManagerServiceRolePolicy
- AWSAutoScalingPlansEC2AutoScalingPolicy
- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupGuardDutyRolePolicyForScans
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupSearchOperatorAccess
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForIndexing
- AWSBackupServiceRolePolicyForItemRestores

- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSBackupServiceRolePolicyForScans
- AWSBatchFullAccess
- AWSBatchServiceEventTargetRole
- AWSBatchServiceRole
- AWSBatchServiceRolePolicyForSageMaker
- AWSBCMDataExportsServiceRolePolicy
- AWSBillingConductorFullAccess
- AWSBillingConductorReadOnlyAccess
- AWSBillingReadOnlyAccess
- AWSBillingServiceRolePolicy
- AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM
- AWSBudgetsActionsWithAWSResourceControlAccess
- AWSBudgetsReadOnlyAccess
- AWSBugBustFullAccess
- AWSBugBustPlayerAccess
- AWSBugBustServiceRolePolicy
- AWSCertificateManagerFullAccess
- AWSCertificateManagerPrivateCAAuditor
- AWSCertificateManagerPrivateCAFullAccess
- AWSCertificateManagerPrivateCAPrivilegedUser
- AWSCertificateManagerPrivateCAReadOnly
- AWSCertificateManagerPrivateCAUser
- AWSCertificateManagerReadOnly
- AWSChatbotServiceLinkedRolePolicy
- AWSCleanRoomsFullAccess
- AWSCleanRoomsFullAccessNoQuerying
- AWSCleanRoomsMLFullAccess

- AWSCleanRoomsMLReadOnlyAccess
- AWSCleanRoomsReadOnlyAccess
- AWSCleanRoomsServiceRolePolicy
- AWSCloud9Administrator
- AWSCloud9EnvironmentMember
- AWSCloud9ServiceRolePolicy
- AWSCloud9SSMInstanceProfile
- AWSCloud9User
- AWSCloudFormationFullAccess
- AWSCloudFormationReadOnlyAccess
- AWSCloudFrontLogger
- AWSCloudFrontVPCOriginServiceRolePolicy
- 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
- AWSCompromisedKeyQuarantineV3
- AWSConfigMultiAccountSetupPolicy
- AWSConfigRemediationServiceRolePolicy
- AWSConfigRoleForOrganizations
- AWSConfigRulesExecutionRole
- AWSConfigServiceRolePolicy
- AWSConfigUserAccess
- AWSConnector
- AWSControlTowerAccountServiceRolePolicy
- AWSControlTowerCloudTrailRolePolicy
- AWSControlTowerIdentityCenterManagementPolicy

- AWSControlTowerServiceRolePolicy
- AWSCostAndUsageReportAutomationPolicy
- AWSDataExchangeDataGrantOwnerFullAccess
- AWSDataExchangeDataGrantReceiverFullAccess
- AWSDataExchangeFullAccess
- AWSDataExchangeProviderFullAccess
- AWSDataExchangeReadOnly
- AWSDataExchangeServiceRolePolicyForLicenseManagement
- AWSDataExchangeServiceRolePolicyForOrganizationDiscovery
- AWSDataExchangeSubscriberFullAccess
- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFullAccess
- AWSDataPipeline_FullAccess
- AWSDataPipeline_PowerUser
- AWSDataSyncDiscoveryServiceRolePolicy
- AWSDataSyncFullAccess
- AWSDataSyncReadOnlyAccess
- AWSDataSyncServiceRolePolicy
- AWSDeadlineCloud-FleetWorker
- AWSDeadlineCloud-UserAccessFarms
- AWSDeadlineCloud-UserAccessFleets
- AWSDeadlineCloud-UserAccessJobs
- AWSDeadlineCloud-UserAccessQueues
- AWSDeadlineCloud-WorkerHost
- AWSDeepLensLambdaFunctionAccessPolicy
- AWSDeepLensServiceRolePolicy
- AWSDeepRacerAccountAdminAccess
- AWSDeepRacerCloudFormationAccessPolicy
- AWSDeepRacerDefaultMultiUserAccess

- AWSDeepRacerFullAccess
- AWSDeepRacerRoboMakerAccessPolicy
- AWSDeepRacerServiceRolePolicy
- AWSDenyAll
- AWSDeviceFarmFullAccess
- AWSDeviceFarmServiceRolePolicy
- AWSDeviceFarmTestGridServiceRolePolicy
- AWSDirectConnectFullAccess
- AWSDirectConnectReadOnlyAccess
- AWSDirectConnectServiceRolePolicy
- AWSDirectoryServiceDataFullAccess
- AWSDirectoryServiceDataReadOnlyAccess
- AWSDirectoryServiceFullAccess
- AWSDirectoryServiceReadOnlyAccess
- AWSDirectoryServiceServiceRolePolicy
- AWSDiscoveryContinuousExportFirehosePolicy
- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy
- AWSEC2CapacityManagerServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSEC2SqlHaInstancePolicy
- AWSEC2SqlHaServiceRolePolicy
- AWSEC2VssSnapshotPolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance

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

- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy
- AWSElasticLoadBalancingServiceRolePolicy
- AWSElementalMediaConnectCreateBridge
- AWSElementalMediaConnectCreateFlow
- AWSElementalMediaConnectDeleteBridge
- AWSElementalMediaConnectDeleteFlow
- AWSElementalMediaConnectFullAccess
- AWSElementalMediaConnectReadOnlyAccess
- 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
- AWSHealthImagingServiceRolePolicy
- AWSHealthOmicsServiceLinkedRolePolicy
- AWSIAMIdentityCenterAllowListForIdentityContext
- AWSIdentityCenterExternalManagementPolicy
- 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
- AWSIoTManagedIntegrationsFullAccess
- AWSIoTManagedIntegrationsRolePolicy
- 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
- AWSLambdaBasicDurableExecutionRolePolicy
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaKinesisExecutionRole
- AWSLambdaManagedEC2ResourceOperator
- AWSLambdaMSKExecutionRole
- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaServiceRolePolicy
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole
- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy
- AWSLicenseManagerMasterAccountRolePolicy
- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedServices_ContactsServiceRolePolicy

- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServices_SelfServiceReporting_ServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy
- AWSManagementConsoleAdministratorAccess
- AWSManagementConsoleBasicUserAccess
- AWSMarketplaceAmiIngestion
- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess
- AWSMarketplaceMeteringRegisterUsage
- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy
- AWSMarketplaceSellerFullAccess
- AWSMarketplaceSellerOfferManagement
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- AWSMcpServiceActionsFullAccess
- AWSMediaConnectServicePolicy
- AWSMediaLiveAnywhereServiceRolePolicy
- AWSMediaTailorServiceRolePolicy
- AWSMigrationHubDiscoveryAccess
- AWSMigrationHubDMSAccess
- AWSMigrationHubFullAccess

- AWSMigrationHubOrchestratorConsoleFullAccess
- AWSMigrationHubOrchestratorInstanceRolePolicy
- AWSMigrationHubOrchestratorPlugin
- AWSMigrationHubOrchestratorServiceRolePolicy
- AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess
- AWSMigrationHubRefactorSpaces-SSMAutomationPolicy
- AWSMigrationHubRefactorSpacesFullAccess
- AWSMigrationHubRefactorSpacesServiceRolePolicy
- AWSMigrationHubSMSAccess
- AWSMigrationHubStrategyCollector
- AWSMigrationHubStrategyConsoleFullAccess
- AWSMigrationHubStrategyServiceRolePolicy
- AWSMobileHub_FullAccess
- AWSMobileHub_ReadOnly
- AWSMSKReplicatorExecutionRole
- AWSNATGatewayServiceRolePolicy
- AWSNetworkFirewallFullAccess
- AWSNetworkFirewallReadOnlyAccess
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess
- AWSNetworkManagerServiceRolePolicy
- AWSObservabilityAdminLogsCentralizationServiceRolePolicy
- AWSObservabilityAdminServiceRolePolicy
- AWSObservabilityAdminTelemetryEnablementServiceRolePolicy
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy

- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPartnerCentralChannelHandshakeApprovalManagement
- AWSPartnerCentralChannelManagement
- AWSPartnerCentralFullAccess
- AWSPartnerCentralMarketingManagement
- AWSPartnerCentralOpportunityManagement
- AWSPartnerCentralSandboxFullAccess
- AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy
- AWSPartnerLedSupportReadOnlyAccess
- AWSPCSComputeNodePolicy
- AWSPCSServiceRolePolicy
- AWSPriceListServiceFullAccess
- AWSPrivateCAAuditor
- AWSPrivateCAConnectorForKubernetesPolicy
- AWSPrivateCAFullAccess
- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly
- AWSPrivateCAUser
- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy

- AWSProtonDeveloperAccess
- AWSProtonFullAccess
- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuickSetupCFGCPacksPermissionsBoundary
- AWSQuickSetupDeploymentRolePolicy
- AWSQuickSetupDevOpsGuruPermissionsBoundary
- AWSQuickSetupDistributorPermissionsBoundary
- AWSQuickSetupEnableAREXExecutionPolicy
- AWSQuickSetupEnableDHMCExecutionPolicy
- AWSQuickSetupJITNADeploymentRolePolicy
- AWSQuickSetupManagedInstanceProfileExecutionPolicy
- AWSQuickSetupManageJITNAResourcesExecutionPolicy
- AWSQuickSetupPatchPolicyBaselineAccess
- AWSQuickSetupPatchPolicyDeploymentRolePolicy
- AWSQuickSetupPatchPolicyPermissionsBoundary
- AWSQuickSetupSchedulerPermissionsBoundary
- AWSQuickSetupSSMDeploymentRolePolicy
- AWSQuickSetupSSMDeploymentS3BucketRolePolicy
- AWSQuickSetupSSMHostMgmtPermissionsBoundary
- AWSQuickSetupSSMLifecycleManagementExecutionPolicy
- AWSQuickSetupSSMManageResourcesExecutionPolicy
- AWSQuickSetupStartSSMAssociationsExecutionPolicy
- AWSQuickSetupStartStopInstancesExecutionPolicy
- AWSQuickSightAssetBundleExportPolicy
- AWSQuickSightAssetBundleImportPolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS

- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightSecretsManagerWriteAccess
- AWSQuickSightSecretsManagerWritePolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess
- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereFullAccess
- AWSRolesAnywhereReadOnly

- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- AWSSecretsManagerClientReadOnlyAccess
- AWSSecurityAgentWebAppPolicy
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSSecurityHubV2ServiceRolePolicy
- AWSSecurityIncidentResponseCaseFullAccess
- AWSSecurityIncidentResponseFullAccess
- AWSSecurityIncidentResponseReadOnlyAccess
- AWSSecurityIncidentResponseServiceRolePolicy
- AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess
- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAIDevOpsPolicy
- AWSServiceRoleForAmazonEKSNodegroup
- AWSServiceRoleForAmazonQDeveloper
- AWSServiceRoleForAWSTransform
- AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

- AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy
- AWSServiceRoleForCodeGuru-Profiler
- AWSServiceRoleForCodeWhispererPolicy
- AWSServiceRoleForEC2ScheduledInstances
- AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy
- AWSServiceRoleForImageBuilder
- AWSServiceRoleForIoTSiteWise
- AWSServiceRoleForLogDeliveryPolicy
- AWSServiceRoleForMonitronPolicy
- AWSServiceRoleForNeptuneGraphPolicy
- AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWSServiceRoleForProcurementInsightsPolicy
- AWSServiceRoleForSMS
- AWSServiceRoleForUserSubscriptions
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting
- AWSServiceRolePolicyForWorkspacesInstances
- AWSShieldDRTAccessPolicy
- AWSShieldServiceRolePolicy
- AWSSocialMessagingServiceRolePolicy
- AWSSSMForSAPServiceLinkedRolePolicy
- AWSSSMOpsInsightsServiceRolePolicy
- AWSSSODirectoryAdministrator
- AWSSSODirectoryReadOnly
- AWSSSOMasterAccountAdministrator
- AWSSSOMemberAccountAdministrator
- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess

- AWSStepFunctionsReadOnlyAccess
- AWSStorageGatewayFullAccess
- AWSStorageGatewayReadOnlyAccess
- AWSStorageGatewayServiceRolePolicy
- AWSSupplyChainFederationAdminAccess
- AWSSupportAccess
- AWSSupportAppFullAccess
- AWSSupportAppReadOnlyAccess
- AWSSupportPlansFullAccess
- AWSSupportPlansReadOnlyAccess
- AWSSupportServiceRolePolicy
- AWSSystemsManagerAccountDiscoveryServicePolicy
- AWSSystemsManagerChangeManagementServicePolicy
- AWSSystemsManagerEnableConfigRecordingExecutionPolicy
- AWSSystemsManagerEnableExplorerExecutionPolicy
- AWSSystemsManagerForSAPFullAccess
- AWSSystemsManagerForSAPReadOnlyAccess
- AWSSystemsManagerJustInTimeAccessServicePolicy
- AWSSystemsManagerJustInTimeAccessTokenPolicy
- AWSSystemsManagerJustInTimeAccessTokenSessionPolicy
- AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy
- AWSSystemsManagerNotificationsServicePolicy
- AWSSystemsManagerOpsDataSyncServiceRolePolicy
- AWSThinkboxAssetServerPolicy
- AWSThinkboxAWSPortalAdminPolicy
- AWSThinkboxAWSPortalGatewayPolicy
- AWSThinkboxAWSPortalWorkerPolicy
- AWSThinkboxDeadlineResourceTrackerAccessPolicy
- AWSThinkboxDeadlineResourceTrackerAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginAdminPolicy

- AWSThinkboxDeadlineSpotEventPluginWorkerPolicy
- AWSTransferConsoleFullAccess
- AWSTransferFullAccess
- AWSTransferLoggingAccess
- AWSTransferReadOnlyAccess
- AWSTransformApplicationDeploymentPolicy
- AWSTransformApplicationECSDeploymentPolicy
- AWSTransformCustomExecuteTransformations
- AWSTransformCustomFullAccess
- AWSTransformCustomManageTransformations
- AWSTransformSecretsManagerConnectorPolicy
- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy
- AWSTrustedAdvisorServiceRolePolicy
- AWSUserAttributeCostAllocationPolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly
- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy
- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy
- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess
- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedDiscoveryServiceRolePolicy

- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess
- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- AWSZoneGroupAccessManagementServiceRolePolicy
- BatchServiceRolePolicy
- BedrockAgentCoreFullAccess
- BedrockAgentCoreNetworkServiceRolePolicy
- BedrockAgentCoreRuntimeIdentityServiceRolePolicy
- Billing
- BudgetsServiceRolePolicy
- CertificateManagerServiceRolePolicy
- ClientVPNServiceConnectionsRolePolicy
- ClientVPNServiceRolePolicy
- CloudFormationStackSetsOrgAdminServiceRolePolicy
- CloudFormationStackSetsOrgMemberServiceRolePolicy
- CloudFrontFullAccess
- CloudFrontReadOnlyAccess
- CloudHSMServiceRolePolicy
- CloudSearchFullAccess
- CloudSearchReadOnlyAccess
- CloudTrailEventContext
- CloudTrailServiceRolePolicy
- CloudWatch-CrossAccountAccess
- CloudWatchActionsEC2Access
- CloudWatchAgentAdminPolicy

- CloudWatchAgentServerPolicy
- CloudWatchApplicationInsightsFullAccess
- CloudWatchApplicationInsightsReadOnlyAccess
- CloudwatchApplicationInsightsServiceLinkedRolePolicy
- CloudWatchApplicationSignalsFullAccess
- CloudWatchApplicationSignalsReadOnlyAccess
- CloudWatchApplicationSignalsServiceRolePolicy
- CloudWatchAutomaticDashboardsAccess
- CloudWatchCrossAccountSharingConfiguration
- CloudWatchEventsBuiltInTargetExecutionAccess
- CloudWatchEventsFullAccess
- CloudWatchEventsInvocationAccess
- CloudWatchEventsReadOnlyAccess
- CloudWatchEventsServiceRolePolicy
- CloudWatchFullAccess
- CloudWatchFullAccessV2
- CloudWatchInternetMonitorFullAccess
- CloudWatchInternetMonitorReadOnlyAccess
- CloudWatchInternetMonitorServiceRolePolicy
- CloudWatchLambdaApplicationSignalsExecutionRolePolicy
- CloudWatchLambdaInsightsExecutionRolePolicy
- CloudWatchLogsAPIKeyAccess
- CloudWatchLogsCrossAccountSharingConfiguration
- CloudWatchLogsFullAccess
- CloudWatchLogsReadOnlyAccess
- CloudWatchNetworkFlowMonitorAgentPublishPolicy
- CloudWatchNetworkFlowMonitorServiceRolePolicy
- CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy
- CloudWatchNetworkMonitorServiceRolePolicy
- CloudWatchOpenSearchDashboardAccess

- CloudWatchOpenSearchDashboardsFullAccess
- CloudWatchReadOnlyAccess
- CloudWatchSyntheticsFullAccess
- CloudWatchSyntheticsReadOnlyAccess
- ComprehendDataAccessRolePolicy
- ComprehendFullAccess
- ComprehendMedicalFullAccess
- ComprehendReadOnly
- ComputeOptimizerAutomationServiceRolePolicy
- ComputeOptimizerReadOnlyAccess
- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy
- ConsoleFullAccessFromVercel
- ConsoleViewOnlyAccessFromVercel
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DeclarativePoliciesEC2Report
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBGlobalTableSettingsManagementServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- EC2FastLaunchFullAccess
- EC2FastLaunchServiceRolePolicy
- EC2FleetTimeShiftableServiceRolePolicy

- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder
- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy
- ECRTemplateServiceRolePolicy
- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess
- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses
- ElementalActivationsReadOnlyAccess
- ElementalAppliancesSoftwareFullAccess
- ElementalAppliancesSoftwareReadOnlyAccess
- ElementalSupportCenterFullAccess
- EMRDescribeClusterPolicyForEMRWAL
- FMSServiceRolePolicy
- FSxDeleteServiceLinkedRoleAccess
- GameLiftContainerFleetPolicy
- GameLiftGameServerGroupPolicy
- GitLabDuoWithAmazonQPermissionsPolicy
- GlobalAcceleratorFullAccess
- GlobalAcceleratorReadOnlyAccess
- GreengrassOTAUpdateArtifactAccess
- GroundTruthSyntheticConsoleFullAccess
- GroundTruthSyntheticConsoleReadOnlyAccess

- Health_OrganizationsServiceRolePolicy
- IAMAccessAdvisorReadOnly
- IAMAccessAnalyzerFullAccess
- IAMAccessAnalyzerReadOnlyAccess
- IAMFullAccess
- IAMReadOnlyAccess
- IAMSelfManageServiceSpecificCredentials
- IAMUserChangePassword
- IAMUserSSHKeys
- IVSFullAccess
- IVSReadOnlyAccess
- IVSRecordToS3
- KafkaConnectServiceRolePolicy
- KafkaServiceRolePolicy
- KeyspacesCDCServiceRolePolicy
- KeyspacesReplicationServiceRolePolicy
- LakeFormationDataAccessServiceRolePolicy
- LexBotPolicy
- LexChannelPolicy
- LightsailExportAccess
- MediaConnectGatewayInstanceRolePolicy
- MediaPackageServiceRolePolicy
- MemoryDBServiceRolePolicy
- MigrationHubDMSAccessServiceRolePolicy
- MigrationHubServiceRolePolicy
- MigrationHubSMSAccessServiceRolePolicy
- MonitronServiceRolePolicy
- MultiPartyApprovalFullAccess
- MultiPartyApprovalReadOnlyAccess

- NeptuneConsoleFullAccess
- NeptuneFullAccess
- NeptuneGraphReadOnlyAccess
- NeptuneReadOnlyAccess
- NetworkAdministrator
- NetworkSecurityDirectorServiceLinkedRolePolicy
- NovaActServiceRolePolicy
- OAMFullAccess
- OAMReadOnlyAccess
- OpensearchIngestionSelfManagedVpcePolicy
- PartnerCentralAccountManagementUserRoleAssociation
- PartnerCentralIncentiveBenefitManagement
- PowerUserAccess
- QAppsServiceRolePolicy
- QBusinessQuicksightPluginPolicy
- QBusinessServiceRolePolicy
- QuickSightAccessForS3StorageManagementAnalyticsReadOnly
- RDSCloudHsmAuthorizationRole
- ReadOnlyAccess
- ResourceGroupsandTagEditorFullAccess
- ResourceGroupsandTagEditorReadOnlyAccess
- ResourceGroupsServiceRolePolicy
- ResourceGroupsTaggingAPITagUntagSupportedResources
- ROSAAmazonEBSCSIDriverOperatorPolicy
- ROSACloudNetworkConfigOperatorPolicy
- ROSAControlPlaneOperatorPolicy
- ROSAImageRegistryOperatorPolicy
- ROSAIngressOperatorPolicy
- ROSAInstallerPolicy
- ROSAKMSProviderPolicy

- ROSAKubeControllerPolicy
- ROSAManageSubscription
- ROSANodePoolManagementPolicy
- ROSASharedVPCEndpointPolicy
- ROSASharedVPCRoute53Policy
- ROSASRESupportPolicy
- ROSAWorkerInstancePolicy
- Route53RecoveryReadinessServiceRolePolicy
- Route53ResolverServiceRolePolicy
- RTBFabricServiceRolePolicy
- S3StorageLensServiceRolePolicy
- SageMakerStudioAdminIAMConsolePolicy
- SageMakerStudioAdminIAMDefaultExecutionPolicy
- SageMakerStudioAdminIAMPermissiveExecutionPolicy
- SageMakerStudioAdminProjectUserRolePolicy
- SageMakerStudioBedrockAgentServiceRolePolicy
- SageMakerStudioBedrockChatAgentUserRolePolicy
- SageMakerStudioBedrockEvaluationJobServiceRolePolicy
- SageMakerStudioBedrockFlowServiceRolePolicy
- SageMakerStudioBedrockFunctionExecutionRolePolicy
- SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy
- SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy
- SageMakerStudioBedrockPromptUserRolePolicy
- SageMakerStudioDomainExecutionRolePolicy
- SageMakerStudioDomainServiceRolePolicy
- SageMakerStudioEMRContainersSystemNamespaceRolePolicy
- SageMakerStudioEMRInstanceRolePolicy
- SageMakerStudioEMRServiceRolePolicy
- SageMakerStudioFullAccess
- SageMakerStudioProjectProvisioningRolePolicy

- SageMakerStudioProjectRoleMachineLearningPolicy
- SageMakerStudioProjectUserRolePermissionsBoundary
- SageMakerStudioProjectUserRolePolicy
- SageMakerStudioQueryExecutionRolePolicy
- SageMakerStudioUserIAMConsolePolicy
- SageMakerStudioUserIAMDefaultExecutionPolicy
- SageMakerStudioUserIAMPermissiveExecutionPolicy
- SecretsManagerReadWrite
- SecurityAgentWebAppAPIPolicy
- SecurityAgentWebAppPolicy
- SecurityAudit
- SecurityLakeResourceManagementServiceRolePolicy
- SecurityLakeServiceLinkedRole
- ServerMigration_ServiceRole
- ServerMigrationConnector
- ServerMigrationServiceConsoleFullAccess
- ServerMigrationServiceLaunchRole
- ServerMigrationServiceRoleForInstanceValidation
- ServiceQuotasFullAccess
- ServiceQuotasReadOnlyAccess
- ServiceQuotasServiceRolePolicy
- SignInLocalDevelopmentAccess
- SimpleWorkflowFullAccess
- SMSVoiceServiceRolePolicy
- SplitCostAllocationDataServiceRolePolicy
- SSMQuickSetupRolePolicy
- SupportUser
- SystemAdministrator
- TranslateFullAccess
- TranslateReadOnly

- ViewOnlyAccess
- VMImportExportRoleForAWSConnector
- VPCLatticeFullAccess
- VPCLatticeReadOnlyAccess
- VPCLatticeServicesInvokeAccess
- WAFLoggingServiceRolePolicy
- WAFRegionalLoggingServiceRolePolicy
- WAFV2LoggingServiceRolePolicy
- WellArchitectedConsoleFullAccess
- WellArchitectedConsoleReadOnlyAccess
- WorkLinkServiceRolePolicy

AccessAnalyzerServiceRolePolicy

描述：允許 Access Analyzer 分析資源中繼資料

`AccessAnalyzerServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 12 月 2 日 17：13 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

政策版本

政策版本： v23 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:GetAccountSetting",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListEntitiesForPolicy",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails",
        "iam:ListAccessKeys",
        "iam:GetLoginProfile",
        "iam:GetAccessKeyLastUsed",
        "iam:ListRolePolicies",
```

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

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AccountManagementFromVercel

描述：與透過 Vercel Marketplace 整合建立的帳戶搭配使用 AWS。提供帳戶管理、通知、成本和用量分析，以及身分提供者管理的存取權。

`AccountManagementFromVercel` 是 AWS 受管政策。

使用此政策

您可以將 `AccountManagementFromVercel` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 12 月 11 日 16：34 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AccountManagementFromVercel`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:CloseAccount",
        "bcm-recommended-actions:ListRecommendedActions",
        "ce:GetCostAndUsage",
        "cur:GetUsageReport",
        "iam:ListSAMLProviders",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSamlProvider",
        "iam:GetSamlProvider"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AdministratorAccess

描述：提供 AWS 服務和資源的完整存取權。

AdministratorAccess 是 AWS 受管政策。

使用此政策

您可以將 AdministratorAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2015 年 2 月 6 日 18：39 UTC
- ARN: arn:aws:iam::aws:policy/AdministratorAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AdministratorAccess-Amplify

描述：授予帳戶管理許可，同時明確允許直接存取 Amplify 應用程式所需的資源。

`AdministratorAccess-Amplify` 是 AWS 受管政策。

使用此政策

您可以將 `AdministratorAccess-Amplify` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 1 日 19：03 UTC
- 編輯時間：2024 年 4 月 4 日，UTC 20：35
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

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

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

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

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

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

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

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

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AdministratorAccess-AWSElasticBeanstalk

描述：授予帳戶管理許可。明確允許開發人員和管理員直接存取管理 AWS Elastic Beanstalk 應用程式所需的資源

AdministratorAccess-AWSElasticBeanstalk 是 AWS 受管政策。

使用此政策

您可以將 AdministratorAccess-AWSElasticBeanstalk 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 1 月 22 日 19：36 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "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",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketOwnershipControls"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AIOpsAssistantIncidentReportPolicy

描述：提供 Amazon AI Operations Assistant 產生調查事件報告所需的許可。

`AIOpsAssistantIncidentReportPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AIOpsAssistantIncidentReportPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- **建立時間**：2025 年 10 月 10 日，UTC 22：04
- **編輯時間**：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantIncidentReportPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GetReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "aiops:GetFact",
        "aiops:ListFacts",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:ListInvestigationEvents",
        "aiops:GetInvestigationEvent"
      ],
      "Resource" : [
        "arn:aws:aiops:*:*:investigation-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AIOpsAssistantPolicy

描述：提供 Amazon AI Operations Assistant 在調查期間分析客戶 AWS 資源所需的 ReadOnly 許可。

`AIOpsAssistantPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AIOpsAssistantPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 2 日 16：21 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantPolicy`

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOPSServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "airflow:List*",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
```

```
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetFunction",
        "appsync:GetGraphqlApi",
        "appsync:GetGraphqlApiEnvironmentVariables",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:List*",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
```

```
            "batch:DescribeSchedulingPolicies",
            "batch:List*",
            "bedrock:GetAgent",
            "bedrock:GetAgentActionGroup",
            "bedrock:GetAgentAlias",
            "bedrock:GetAgentKnowledgeBase",
            "bedrock:GetDataSource",
            "bedrock:GetGuardrail",
            "bedrock:GetKnowledgeBase",
            "bedrock:List*",
            "budgets:Describe*",
            "budgets:List*",
            "ce:Describe*",
            "ce:GetAnomalyMonitors",
            "ce:GetAnomalySubscriptions",
            "ce:List*",
            "chatbot:Describe*",
            "chatbot:GetMicrosoftTeamsChannelConfiguration",
            "chatbot:List*",
            "cleanrooms-ml:GetTrainingDataset",
            "cleanrooms-ml:List*",
            "cleanrooms:GetAnalysisTemplate",
            "cleanrooms:GetCollaboration",
            "cleanrooms:GetConfiguredTable",
            "cleanrooms:GetConfiguredTableAnalysisRule",
            "cleanrooms:GetConfiguredTableAssociation",
            "cleanrooms:GetMembership",
            "cleanrooms:List*",
            "cloudformation:Describe*",
            "cloudformation:GetResource",
            "cloudformation:GetStackPolicy",
            "cloudformation:GetTemplate",
            "cloudformation:List*",
            "cloudfront:Describe*",
            "cloudfront:GetCachePolicy",
            "cloudfront:GetCloudFrontOriginAccessIdentity",
            "cloudfront:GetContinuousDeploymentPolicy",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:GetFunction",
            "cloudfront:GetKeyGroup",
            "cloudfront:GetMonitoringSubscription",
            "cloudfront:GetOriginAccessControl",
            "cloudfront:GetOriginRequestPolicy",
```

```
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartQuery",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetInsightRuleReport",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetService",
        "cloudwatch:GetServiceLevelObjective",
        "cloudwatch:List*",
        "codeartifact:Describe*",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:List*",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:List*",
```

```
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:List*",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:List*",
        "codestar-notifications:Describe*",
        "codestar-notifications:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListTagsForResource",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect:Describe*",
        "connect:GetTaskTemplate",
        "connect:List*",
        "databrew:Describe*",
        "databrew:List*",
```

```
        "datapipeline:Describe*",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:List*",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetStorageProfile",
        "deadline:List*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:GetResourceCollection",
        "devops-guru:List*",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:Describe*",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
```

```
            "ec2:GetVerifiedAccessInstanceWebAcl",
            "ec2:SearchLocalGatewayRoutes",
            "ec2:SearchTransitGatewayRoutes",
            "ecr:Describe*",
            "ecr:GetLifecyclePolicy",
            "ecr:GetRegistryPolicy",
            "ecr:GetRepositoryPolicy",
            "ecr:List*",
            "ecs:Describe*",
            "ecs:List*",
            "eks:Describe*",
            "eks:List*",
            "elasticache:Describe*",
            "elasticache:List*",
            "elasticbeanstalk:Describe*",
            "elasticbeanstalk:List*",
            "elasticfilesystem:Describe*",
            "elasticloadbalancing:GetResourcePolicy",
            "elasticloadbalancing:GetTrustStoreCaCertificatesBundle",
            "elasticloadbalancing:GetTrustStoreRevocationContent",
            "elasticloadbalancing:Describe*",
            "elasticmapreduce:Describe*",
            "elasticmapreduce:List*",
            "emr-containers:Describe*",
            "emr-containers:List*",
            "emr-serverless:GetApplication",
            "emr-serverless:List*",
            "es:Describe*",
            "es:List*",
            "events:Describe*",
            "events:List*",
            "evidently:GetExperiment",
            "evidently:GetFeature",
            "evidently:GetLaunch",
            "evidently:GetProject",
            "evidently:GetSegment",
            "evidently:List*",
            "firehose:Describe*",
            "firehose:List*",
            "fis:GetExperimentTemplate",
            "fis:GetTargetAccountConfiguration",
            "fis:List*",
            "fms:GetNotificationChannel",
            "fms:GetPolicy",
```

```
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "frauddetector:BatchGetVariable",
        "frauddetector:Describe*",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:List*",
        "glue:querySchemaVersionMetadata",
        "grafana:Describe*",
        "grafana:List*",
        "greengrass:Describe*",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:List*",
        "guardduty:GetDetector",
```

```
            "guardduty:GetFilter",
            "guardduty:GetIPSet",
            "guardduty:GetMalwareProtectionPlan",
            "guardduty:GetMasterAccount",
            "guardduty:GetMembers",
            "guardduty:GetThreatIntelSet",
            "guardduty:List*",
            "health:DescribeEvents",
            "health:DescribeEventDetails",
            "healthlake:Describe*",
            "healthlake:List*",
            "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:GetUser",
            "iam:GetUserPolicy",
            "iam:ListAttachedRolePolicies",
            "iam:ListOpenIDConnectProviders",
            "iam:ListRolePolicies",
            "iam:ListRoles",
            "iam:ListServerCertificates",
            "iam:ListVirtualMFADevices",
            "identitystore:DescribeGroup",
            "identitystore:DescribeGroupMembership",
            "identitystore:ListGroupMemberships",
            "identitystore:ListGroups",
            "imagebuilder:GetComponent",
            "imagebuilder:GetContainerRecipe",
            "imagebuilder:GetDistributionConfiguration",
            "imagebuilder:GetImage",
            "imagebuilder:GetImagePipeline",
            "imagebuilder:GetImageRecipe",
            "imagebuilder:GetInfrastructureConfiguration",
            "imagebuilder:GetLifecyclePolicy",
            "imagebuilder:GetWorkflow",
```

```
        "imagebuilder:List*",
        "inspector2:List*",
        "inspector:Describe*",
        "inspector:List*",
        "internetmonitor:GetMonitor",
        "internetmonitor:List*",
        "iot:Describe*",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotfleethub:Describe*",
        "iotfleethub:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:List*",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:List*",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:List*",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
```

```
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeKey",
        "kms:ListResourceTags",
        "kms:ListKeys",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeyRotations",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:GetResourceLFTags",
        "lakeformation:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "lex:Describe*",
        "lex:List*",
        "license-manager:GetLicense",
        "license-manager:List*",
        "lightsail:GetAlarms",
```

```
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:List*",
        "lookoutvision:Describe*",
        "lookoutvision:List*",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:List*",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
        "macie2:List*",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:GetCloudWatchAlarmTemplate",
```

```
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
        "nimble:GetLaunchProfile",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:List*",
```

```
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:List*",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:List*",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:List*",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:List*",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:Describe*",
        "pipes:List*",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:List*",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
```

```
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:List*",
        "qldb:Describe*",
        "qldb:List*",
        "ram:GetPermission",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:List*",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
```

```
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:List*",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:List*",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
```

```
            "s3:GetBucketTagging",
            "s3:GetBucketVersioning",
            "S3:GetBucketWebsite",
            "s3:GetEncryptionConfiguration",
            "s3:GetIntelligentTieringConfiguration",
            "s3:GetInventoryConfiguration",
            "s3:GetLifecycleConfiguration",
            "s3:GetMetricsConfiguration",
            "s3:GetMultiRegionAccessPoint",
            "s3:GetMultiRegionAccessPointPolicy",
            "s3:GetMultiRegionAccessPointPolicyStatus",
            "s3:GetReplicationConfiguration",
            "s3:GetStorageLensConfiguration",
            "s3:GetStorageLensConfigurationTagging",
            "s3:GetStorageLensGroup",
            "s3:List*",
            "sagemaker:Describe*",
            "sagemaker:List*",
            "scheduler:GetSchedule",
            "scheduler:GetScheduleGroup",
            "scheduler:List*",
            "schemas:Describe*",
            "schemas:GetResourcePolicy",
            "schemas:List*",
            "secretsmanager:Describe*",
            "secretsmanager:GetResourcePolicy",
            "secretsmanager:List*",
            "securityhub:BatchGetAutomationRules",
            "securityhub:BatchGetSecurityControls",
            "securityhub:Describe*",
            "securityhub:GetConfigurationPolicy",
            "securityhub:GetConfigurationPolicyAssociation",
            "securityhub:GetEnabledStandards",
            "securityhub:GetFindingAggregator",
            "securityhub:GetInsights",
            "securityhub:List*",
            "securitylake:GetSubscriber",
            "securitylake:List*",
            "servicecatalog:Describe*",
            "servicecatalog:GetApplication",
            "servicecatalog:GetAttributeGroup",
            "servicecatalog:List*",
            "servicequotas:GetServiceQuota",
            "ses:Describe*",
```

```
            "ses:GetAccount",
            "ses:GetAddonInstance",
            "ses:GetAddonSubscription",
            "ses:GetArchive",
            "ses:GetConfigurationSet",
            "ses:GetConfigurationSetEventDestinations",
            "ses:GetContactList",
            "ses:GetDedicatedIpPool",
            "ses:GetDedicatedIps",
            "ses:GetEmailIdentity",
            "ses:GetEmailTemplate",
            "ses:GetIngressPoint",
            "ses:GetRelay",
            "ses:GetRuleSet",
            "ses:GetTemplate",
            "ses:GetTrafficPolicy",
            "ses:List*",
            "shield:Describe*",
            "shield:List*",
            "signer:GetSigningProfile",
            "signer:List*",
            "sns:GetDataProtectionPolicy",
            "sns:GetSubscriptionAttributes",
            "sns:GetTopicAttributes",
            "sns:List*",
            "sqs:GetQueueAttributes",
            "sqs:GetQueueUrl",
            "sqs:List*",
            "ssm-contacts:GetContact",
            "ssm-contacts:GetContactChannel",
            "ssm-contacts:List*",
            "ssm-incidents:GetReplicationSet",
            "ssm-incidents:GetResponsePlan",
            "ssm-incidents:List*",
            "ssm-sap:GetApplication",
            "ssm-sap:List*",
            "ssm:Describe*",
            "ssm:GetDefaultPatchBaseline",
            "ssm:GetDocument",
            "ssm:GetParameters",
            "ssm:GetPatchBaseline",
            "ssm:GetResourcePolicies",
            "ssm:List*",
            "sso-directory:SearchGroups",
```

```
            "sso-directory:SearchUsers",
            "sso:GetInlinePolicyForPermissionSet",
            "sso:GetManagedApplicationInstance",
            "sso:GetPermissionsBoundaryForPermissionSet",
            "sso:GetSharedSsoConfiguration",
            "sso:ListAccountAssignments",
            "sso:ListApplicationAssignments",
            "sso:ListApplications",
            "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
            "sso:ListInstances",
            "sso:ListManagedPoliciesInPermissionSet",
            "sso:ListTagsForResource",
            "states:GetExecutionHistory",
            "states:Describe*",
            "states:List*",
            "synthetics:Describe*",
            "synthetics:GetCanary",
            "synthetics:GetGroup",
            "synthetics:List*",
            "tag:GetResources",
            "timestream:Describe*",
            "timestream:List*",
            "transfer:Describe*",
            "transfer:List*",
            "verifiedpermissions:GetIdentitySource",
            "verifiedpermissions:GetPolicy",
            "verifiedpermissions:GetPolicyStore",
            "verifiedpermissions:GetPolicyTemplate",
            "verifiedpermissions:GetSchema",
            "verifiedpermissions:List*",
            "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:List*",
            "wafv2:GetIPSet",
            "wafv2:GetLoggingConfiguration",
            "wafv2:GetRegexPatternSet",
```

```
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:List*",
        "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:List*",
        "workspaces:Describe*",
        "xray:BatchGetTraces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSS3AccessForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amplify",
        "arn:aws:s3:::cdk--assets--*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ViaAWSService" : [
            "amplify.amazonaws.com"
          ],
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AIOPSAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AIOpsConsoleAdminPolicy

描述：透過 AWS 主控台授予 Amazon AI Operations 服務及其必要許可的完整存取權。它還包含使用身分感知主控台工作階段的許可。

AIOpsConsoleAdminPolicy 是 AWS 受管政策。

使用此政策

您可以將 AIOpsConsoleAdminPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 12 月 2 日 23：51 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AIOpsConsoleAdminPolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        }
      }
    },
    {
      "Sid" : "SSOApplicationTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:TagResource"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/aiops"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:RequestTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "SSOTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:TagResource"
      ],
      "Resource" : "arn:aws:sso::*:application/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:ListApplications",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:GetSSOStatus",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
```

```
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "IdentityPropagationAccess",
      "Effect" : "Allow",
      "Action" : [
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudtrailAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListEventDataStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMIntegrationSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:aws/ssm/3p/*"
    },
    {
      "Sid" : "SSMIntegrationAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
```

```
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationCreatePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/service-role/
AWSServiceRoleSSMIntegrationsPolicy*"
    },
    {
      "Sid" : "ChatbotConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackWorkspaces",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleToAIOps",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "aiops.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "TagBoundaryPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleToSSMIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.integrations.amazonaws.com"
        },
        "ArnEquals" : {
          "iam:AssociatedResourceArn" : "arn:aws:aiops:*:*:investigation-group/*"
        }
      }
    },
    {
      "Sid" : "SSMOpsItemAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:*:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : "CloudWatch",
          "aws:ResourceTag/Integration" : "CloudWatch"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Integration"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "CreateAIOpsCrossAccountAssistantPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/AIOpsCrossAccountAssistantPolicy*"
    },
    {
      "Sid" : "AmazonQAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AIOpsOperatorAccess

描述：授予 Amazon AI Operations APIs 的存取權，以建立、更新和刪除調查、調查事件和調查資源。它還包含所有 AI 操作 APIs ReadOnly 存取權。

`AIOpsOperatorAccess` 是 AWS 受管政策。

使用此政策

您可以將 AIOpsOperatorAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 2 日 23：51 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AIOpsOperatorAccess

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsOperatorAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:CreateInvestigation",
        "aiops:CreateInvestigationEvent",
        "aiops:CreateInvestigationResource",
        "aiops:DeleteInvestigation",
        "aiops:Get*",
        "aiops:List*",
        "aiops:UpdateInvestigation",
        "aiops:UpdateInvestigationEvent",
        "aiops:ValidateInvestigationGroup",
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
```

```
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMSettingServiceIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationTagAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
      }
    },
    {
      "Sid" : "SSMOpsItemIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        }
      }
    },
    {
      "Sid" : "SSMTagOperation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
      }
```

```
    },
    {
      "Sid" : "SSMOpsSummaryIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AIOpsReadOnlyAccess

描述：授予 Amazon AI Operations 服務及其必要資源的 ReadOnly 許可。

`AIOpsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AIOpsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 2 日 23：51 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsReadOnlyAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:Get*",
        "aiops:List*",
        "aiops:ValidateInvestigationGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AlexaForBusinessDeviceSetup

描述：提供 AlexaForBusiness 服務的裝置設定存取權

AlexaForBusinessDeviceSetup 是 AWS 受管政策。

使用此政策

您可以將 AlexaForBusinessDeviceSetup 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 30 日 16：47 UTC
- 編輯時間：2019 年 5 月 20 日，UTC 21：05
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AlexaForBusinessFullAccess

描述：授予對 AlexaForBusiness 資源的完整存取權，以及對相關 的存取權 AWS 服務

`AlexaForBusinessFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AlexaForBusinessFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 30 日 16：47 UTC
- 編輯時間：2020 年 7 月 1 日，UTC 21：01
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AlexaForBusinessGatewayExecution

描述：提供 AlexaForBusiness 服務的閘道執行存取權

AlexaForBusinessGatewayExecution 是 AWS 受管政策。

使用此政策

您可以將 AlexaForBusinessGatewayExecution 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- **建立時間**：2017 年 11 月 30 日 16：47 UTC
- **編輯時間**：2017 年 11 月 30 日 16：47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AlexaForBusinessLifesizeDelegatedAccessPolicy

描述：提供對 Lifesize AVS 裝置的存取

`AlexaForBusinessLifesizeDelegatedAccessPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AlexaForBusinessLifesizeDelegatedAccessPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 6 月 4 日 19：46 UTC
- 編輯時間：2020 年 6 月 12 日 20：31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A2IWO7UEGWV4TL"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "a4b:SearchDevices"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "a4b:filters_deviceType" : [
            "*A2IWO7UEGWV4TL"
          ]
        },
        "Null" : {
          "a4b:filters_deviceType" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL",
        "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/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AlexaForBusinessNetworkProfileServicePolicy

描述：此政策可讓 Alexa for Business 執行網路設定檔排程的自動化任務。

`AlexaForBusinessNetworkProfileServicePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 3 月 13 日 00：53 UTC

- **編輯時間**：2019 年 4 月 5 日，UTC 21：57
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AlexaForBusinessPolyDelegatedAccessPolicy

描述：提供 Poly AVS 裝置的存取權

AlexaForBusinessPolyDelegatedAccessPolicy 是 AWS 受管政策。

使用此政策

您可以將 AlexaForBusinessPolyDelegatedAccessPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 10 月 16 日 19：48 UTC
- 編輯時間：2019 年 10 月 16 日 19：48 UTC
- ARN: arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
```

```
        "a4b:GetDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD"
      ]
    },
    {
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A238TWV36W3S92",
            "A1FUZ1SC53VJXD"
          ]
        }
      }
    },
    {
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AlexaForBusinessReadOnlyAccess

描述：提供 AlexaForBusiness 服務的唯讀存取權

`AlexaForBusinessReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AlexaForBusinessReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 30 日 16：47 UTC
- 編輯時間：2019 年 11 月 20 日 00：25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAPIGatewayAdministrator

描述：提供透過 在 Amazon APIs Gateway 中create/edit/delete API 的完整存取權 AWS 管理主控台。Amazon API Gateway

AmazonAPIGatewayAdministrator 是 AWS 受管政策。

使用此政策

您可以將 AmazonAPIGatewayAdministrator 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 7 月 9 日 17：34 UTC
- 編輯時間：2015 年 7 月 9 日 17：34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAPIGatewayInvokeFullAccess

描述：提供在 Amazon API Gateway APIs中叫用 API 的完整存取權。

`AmazonAPIGatewayInvokeFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonAPIGatewayInvokeFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 7 月 9 日 17：36 UTC
- 編輯時間：2018 年 12 月 18 日 18：25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonAPIGatewayPushToCloudWatchLogs

描述：允許 API Gateway 將日誌推送至使用者帳戶。

AmazonAPIGatewayPushToCloudWatchLogs 是 AWS 受管政策。

使用此政策

您可以將 AmazonAPIGatewayPushToCloudWatchLogs 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 11 月 11 日 23：41 UTC
- 編輯時間：2015 年 11 月 11 日 23：41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAppFlowFullAccess

描述：提供 Amazon AppFlow 的完整存取權，以及流量來源或目的地 (S3 和 Redshift) 支援的 AWS 服務存取權。也提供存取 KMS 以進行加密

AmazonAppFlowFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonAppFlowFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 6 月 2 日 23：30 UTC
- 編輯時間：2022 年 2 月 28 日 23：11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonAppFlowReadOnlyAccess

描述：提供 Amazon Appflow 流程的唯讀存取權

AmazonAppFlowReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonAppFlowReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 6 月 2 日，23：26 UTC
- 編輯時間：2022 年 2 月 28 日 20：42 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

描述：授予 ARC 區域切換的許可，以進行計劃執行和計劃評估。

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy 是 AWS 受管政策。

使用此政策

您可以
將 AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 3 日 19：34 UTC
- 編輯時間：2026 年 3 月 5 日 19：27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-region-switch:GetPlan",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListPlanExecutions"
      ],
      "Resource" : "*",
      "Sid" : "GetPlanAndExecutions"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:SimulatePrincipalPolicy",
```

```
      "Resource" : "arn:aws:iam::*:role/*",
      "Sid" : "PlanEvaluation"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*",
      "Sid" : "CloudWatch"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAppStreamFullAccess

描述：透過 提供 Amazon AppStream 的完整存取權 AWS 管理主控台。

`AmazonAppStreamFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonAppStreamFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2020 年 8 月 28 日 17：24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAppStreamPCAAccess

描述：Amazon AppStream 2.0 存取客戶帳戶中的 AWS Certificate Manager Private CA 以進行憑證型身分驗證

AmazonAppStreamPCAAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonAppStreamPCAAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 10 月 24 日 17：05 UTC
- 編輯時間：2022 年 10 月 24 日 17：05 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAppStreamReadOnlyAccess

描述：透過 提供 Amazon AppStream 的唯讀存取權 AWS 管理主控台。

`AmazonAppStreamReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonAppStreamReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonAppStreamServiceAccess

描述：Amazon AppStream 服務角色的預設政策。

AmazonAppStreamServiceAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonAppStreamServiceAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 11 月 19 日 04：17 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "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-*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAthenaFullAccess

描述：提供 Amazon Athena 的完整存取權，以及啟用查詢、寫入結果和資料管理所需的相依性範圍存取權。

AmazonAthenaFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonAthenaFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 11 月 30 日 16：46 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
```

```
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:StartColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetCatalogImportStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseQueryResultsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Sid" : "BaseAthenaExamplesPermissions",
      "Effect" : "Allow",
      "Action" : [
```

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonAthenaServiceRolePolicy

描述：允許存取執行 Amazon Athena 所需的其他 AWS 服務資源

AmazonAthenaServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 11 月 14 日 22：34 UTC
- 編輯時間：2025 年 11 月 14 日 22：34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonAthenaServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Athena",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonAugmentedAIFullAccess

描述：提供執行所有操作的存取權 Amazon 增強版 AI 資源，包括 FlowDefinitions、HumanTaskUis 和 HumanLoops。不允許針對公有群眾工作團隊建立 FlowDefinitions 的存取權。

`AmazonAugmentedAIFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonAugmentedAIFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 16：21 UTC
- 編輯時間：2019 年 12 月 3 日 16：21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAugmentedAIHumanLoopFullAccess

描述：提供在 HumanLoops 上執行所有操作的存取權。

`AmazonAugmentedAIHumanLoopFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonAugmentedAIHumanLoopFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 16：20 UTC
- 編輯時間：2019 年 12 月 3 日 16：20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAugmentedAIIntegratedAPIAccess

描述：提供執行所有操作的存取權 Amazon 增強版 AI 資源，包括 FlowDefinitions、HumanTaskUis 和 HumanLoops。也可讓您存取與 Amazon 增強版 AI 整合的服務操作。

`AmazonAugmentedAIIntegratedAPIAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonAugmentedAIIntegratedAPIAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 4 月 22 日，20：47 UTC
- 編輯時間：2020 年 4 月 22 日，20：47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonAuroraDSQLConsoleFullAccess

描述：提供主控台對 Aurora DSQL 的完整管理存取權

AmazonAuroraDSQLConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonAuroraDSQLConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2024 年 12 月 3 日 15：36 UTC
- **編輯時間**：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLConsoleFullAccess`

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
```

```
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DsqlConsolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ValidatePolicy",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    },
    {
```

```
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonAuroraDSQLFullAccess

描述：提供 Aurora DSQL 的完整管理存取權

AmazonAuroraDSQLFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonAuroraDSQLFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 12 月 3 日 15：36 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAuroraDSQLFullAccess

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSDescribePermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonAuroraDSQLReadOnlyAccess

描述：提供 Aurora DSQL 的唯讀存取權

AmazonAuroraDSQLReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonAuroraDSQLReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 3 日 15：21 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonAuroraDSQLReadOnlyAccess

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetClusterPolicy",
        "dsql:GetCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRo

描述：提供 Bedrock 代理程式核心記憶體的 Bedrock Model 推論許可

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy 是 AWS 受管政策。

使用此政策

您可以
將 AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 7 月 16 日 13：37 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBedrockFullAccess

描述：提供 Amazon Bedrock 的完整存取權，以及對 Amazon Bedrock 所需相關服務的有限存取權

`AmazonBedrockFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonBedrockFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 12 月 6 日 15：47 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "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" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
```

```
        },
        "StringLike" : {
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
```

```
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
```

```
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBedrockLimitedAccess

描述：提供對 Amazon Bedrock 及其所需相關服務的有限存取權

AmazonBedrockLimitedAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonBedrockLimitedAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 6 月 29 日，UTC 22：22
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*",
        "bedrock:CallWithBearerToken",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreateInferenceProfile",
        "bedrock:CreateModelCopyJob",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
        "bedrock:CreatePromptRouter",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:DeleteCustomModel",
        "bedrock:DeleteGuardrail",
        "bedrock:DeleteImportedModel",
        "bedrock:DeleteInferenceProfile",
        "bedrock:DeletePromptRouter",
        "bedrock:DeleteProvisionedModelThroughput",
        "bedrock:StopEvaluationJob",
        "bedrock:StopModelCustomizationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:TagResource",
        "bedrock:UntagResource",
        "bedrock:UpdateGuardrail",
        "bedrock:UpdateProvisionedModelThroughput",
```

```
        "bedrock:ApplyGuardrail",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "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" : "BedrockMantleAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBedrockMantleFullAccess

描述：提供對 Amazon Bedrock Mantle 的完整存取權，以及對其所需相關服務的有限存取權

`AmazonBedrockMantleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonBedrockMantleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 12 月 4 日 07：19 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonBedrockMantleInferenceAccess

描述：提供對 Amazon Bedrock Mantle 的讀取和推論建立存取權

`AmazonBedrockMantleInferenceAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonBedrockMantleInferenceAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- 建立時間：2025 年 12 月 4 日 07：19 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleInferenceAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleInference",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBedrockMantleReadOnly

描述：提供對 Amazon Bedrock Mantle 的唯讀存取權

AmazonBedrockMantleReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonBedrockMantleReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 12 月 4 日 07：19 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockMantleReadOnly

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:Get*",
```

```
        "bedrock-mantle:List*"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBedrockMarketplaceAccess

描述：提供對 Amazon Bedrock Marketplace 及其所需相關服務的有限存取權

AmazonBedrockMarketplaceAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonBedrockMarketplaceAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 6 月 29 日，UTC 22：22
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockMarketplaceAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMarketplaceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:DeleteMarketplaceModelEndpoint",
        "bedrock:DeregisterMarketplaceModelEndpoint",
        "bedrock:RegisterMarketplaceModelEndpoint",
        "bedrock:UpdateMarketplaceModelEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
```

```
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBedrockReadOnly

描述：提供 Amazon Bedrock 的唯讀存取權

AmazonBedrockReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonBedrockReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 12 月 6 日 15：48 UTC

- **編輯時間**：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBedrockStudioPermissionsBoundary

描述：定義 Amazon Bedrock Studio 為操作 Amazon Bedrock Studio 資源而建立的 IAM 角色的最大許可。

AmazonBedrockStudioPermissionsBoundary 是 AWS 受管政策。

使用此政策

您可以將 AmazonBedrockStudioPermissionsBoundary 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 8 月 1 日 00：24 UTC
- 編輯時間：2024 年 8 月 1 日 00：24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBedrockStudioPermissionsBoundary

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::br-studio-${aws:PrincipalAccount}-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AccessOpenSearchCollections",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*::foundation-model/*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:ListTagsForResource",
        "bedrock:TagResource",
        "bedrock:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RetrieveAndGenerate",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "WriteLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/br-studio-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "InvokeLambdaFunctions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:br-studio-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
```

```
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretsManagerSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:br-studio/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "UseKmsKeyWithBedrock",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "UseKmsKeyWithAwsServices",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBraketFullAccess

描述：透過 AWS 管理主控台 和 SDK 提供 Amazon Braket 的完整存取權。也提供相關服務的存取權（例如 S3、日誌）。

AmazonBraketFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonBraketFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 8 月 6 日，20：12 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "servicequotas:GetServiceQuota",
```

```
        "cloudwatch:GetMetricData",
        "pricing:GetProducts"
      ],
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonBraketJobsExecutionPolicy

描述：授予執行 Amazon Braket 任務所需的 AWS 服務 和資源的存取權，包括 S3、Cloudwatch、IAM 和 Braket

`AmazonBraketJobsExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 AmazonBraketJobsExecutionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 11 月 26 日 19：34 UTC
- 編輯時間：2021 年 11 月 28 日 05：34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonBraketServiceRolePolicy

描述：允許 Amazon Braket 代表您建立和管理 AWS 資源

AmazonBraketServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 8 月 4 日 17：12 UTC
- 編輯時間：2025 年 7 月 11 日 21：37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonChimeFullAccess

描述：透過 提供 Amazon Chime Admin Console 的完整存取權 AWS 管理主控台。

AmazonChimeFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonChimeFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 11 月 1 日，UTC 22：15
- 編輯時間：2020 年 12 月 14 日，21：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonChimeReadOnly

描述：透過 提供 Amazon Chime Admin Console 的唯讀存取權 AWS 管理主控台。

AmazonChimeReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonChimeReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 11 月 1 日 22：04 UTC
- 編輯時間：2020 年 12 月 14 日，20：53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonChimeSDK

描述：提供 Amazon Chime SDK 操作的存取權

AmazonChimeSDK 是 AWS 受管政策。

使用此政策

您可以將 AmazonChimeSDK 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 2 月 4 日，UTC 21：53
- 編輯時間：2023 年 1 月 10 日 18：05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeSDK

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

描述：Amazon Chime SDK MediaPipelines Service 連結角色的受管政策

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 4 月 4 日，UTC 22：02
- 編輯時間：2023 年 12 月 8 日 19：14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonChimeSDKMessagingServiceRolePolicy

描述：允許 Amazon Chime SDK 傳訊存取 AWS 資源並啟用傳訊功能

AmazonChimeSDKMessagingServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 3 月 3 日 01：43 UTC
- 編輯時間：2023 年 3 月 3 日 01：43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonChimeServiceRolePolicy

描述：允許存取 Amazon Chime 使用或管理 AWS 的資源

AmazonChimeServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 9 月 30 日，UTC 22：25
- 編輯時間：2019 年 9 月 30 日，UTC 22：25
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonChimeTranscriptionServiceLinkedRolePolicy

描述：允許 Amazon Chime 代表您存取 Amazon Transcribe 和 Amazon Transcribe Medical

`AmazonChimeTranscriptionServiceLinkedRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 8 月 4 日，UTC 21：47
- 編輯時間：2021 年 8 月 4 日 21：47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonChimeUserManagement

描述：透過 提供 Amazon Chime Admin Console 的使用者管理存取權 AWS 管理主控台。

AmazonChimeUserManagement 是 AWS 受管政策。

使用此政策

您可以將 AmazonChimeUserManagement 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 1 日 22：17 UTC
- 編輯時間：2020 年 2 月 18 日 19：26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonChimeUserManagement

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

描述：Amazon Chime VoiceConnector 的服務連結角色受管政策

AmazonChimeVoiceConnectorServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 9 月 30 日，UTC 22：16
- 編輯時間：2023 年 4 月 14 日 21：49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCloudDirectoryFullAccess

描述：提供 Amazon Cloud Directory Service 的完整存取權。

`AmazonCloudDirectoryFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCloudDirectoryFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 2 月 25 日 00：41 UTC
- 編輯時間：2017 年 2 月 25 日 00：41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCloudDirectoryReadOnlyAccess

描述：提供 Amazon Cloud Directory Service 的唯讀存取權。

`AmazonCloudDirectoryReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCloudDirectoryReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 2 月 28 日 23：42 UTC
- 編輯時間：2017 年 2 月 28 日 23：42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCloudWatchEvidentlyFullAccess

描述：僅提供 Amazon CloudWatch Evidently 的完整存取權。也提供對相關 Amazon S3、Amazon SNS、Amazon CloudWatch 和其他相關服務的存取權。

`AmazonCloudWatchEvidentlyFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCloudWatchEvidentlyFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 29 日 15：10 UTC
- 編輯時間：2021 年 11 月 29 日 15：10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonCloudWatchEvidentlyReadOnlyAccess

描述：提供 Amazon CloudWatch Evidently 的唯讀存取權

`AmazonCloudWatchEvidentlyReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCloudWatchEvidentlyReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 29 日 15：08 UTC
- 編輯時間：2021 年 11 月 29 日 15：08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonCloudWatchEvidentlyServiceRolePolicy

描述：允許 CloudWatch Evidently Service 代表客戶管理相關聯的 AWS 資源

`AmazonCloudWatchEvidentlyServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 9 月 13 日 17：25 UTC
- 編輯時間：2022 年 9 月 13 日 17：25 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCloudWatchRUMFullAccess

描述：授予 Amazon CloudWatch RUM 服務的完整存取許可

AmazonCloudWatchRUMFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonCloudWatchRUMFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 29 日 15：46 UTC
- 編輯時間：2021 年 11 月 29 日 15：46 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonCloudWatchRUMReadOnlyAccess

描述：授予 Amazon CloudWatch RUM 服務的唯讀許可

`AmazonCloudWatchRUMReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCloudWatchRUMReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 29 日 15：43 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetResourcePolicy",
        "rum:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanariesLastRun",
        "synthetics:describeCanaries"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonCloudWatchRUMServiceRolePolicy

描述：准許 Amazon CloudWatch RUM Service 將監控資料發佈至其他相關 AWS 服務

`AmazonCloudWatchRUMServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 17 日 23：17 UTC
- 編輯時間：2023 年 2 月 22 日 20：35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeCatalystFullAccess

描述：提供 Amazon CodeCatalyst 的完整存取權

AmazonCodeCatalystFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonCodeCatalystFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 4 月 20 日 16：50 UTC
- 編輯時間：2023 年 4 月 20 日 16：50 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeCatalystReadOnlyAccess

描述：提供 Amazon CodeCatalyst 的唯讀存取權

`AmazonCodeCatalystReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCodeCatalystReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 4 月 20 日 16：49 UTC
- 編輯時間：2023 年 4 月 20 日 16：49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeCatalystSupportAccess

描述：允許 Amazon CodeCatalyst 代表您建立、更新和解決 AWS 支援 案例。

`AmazonCodeCatalystSupportAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCodeCatalystSupportAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 4 月 20 日 12：34 UTC
- 編輯時間：2023 年 4 月 20 日 12：34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeGuruProfilerAgentAccess

描述：提供 Amazon CodeGuru Profiler 代理程式所需的存取權。

`AmazonCodeGuruProfilerAgentAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCodeGuruProfilerAgentAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 2 月 5 日，UTC 22：11
- 編輯時間：2022 年 5 月 5 日 18：11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeGuruProfilerFullAccess

描述：提供 Amazon CodeGuru Profiler 的完整存取權。

`AmazonCodeGuruProfilerFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCodeGuruProfilerFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 10：13 UTC
- 編輯時間：2020 年 7 月 15 日 03：23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeGuruProfilerReadOnlyAccess

描述：提供 Amazon CodeGuru Profiler 的唯讀存取權。

`AmazonCodeGuruProfilerReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCodeGuruProfilerReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 10：30 UTC
- 編輯時間：2020 年 6 月 27 日 23：52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeGuruReviewerFullAccess

描述：授予對 Amazon CodeGuru Reviewer 的完整存取權，以及對必要相依性的範圍存取權。

`AmazonCodeGuruReviewerFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCodeGuruReviewerFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 08：33 UTC
- 編輯時間：2020 年 8 月 29 日 04：16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeGuruReviewerReadOnlyAccess

描述：提供 Amazon CodeGuru Reviewer 的唯讀存取權。

`AmazonCodeGuruReviewerReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonCodeGuruReviewerReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 08：48 UTC
- 編輯時間：2020 年 8 月 29 日 04：15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonCodeGuruReviewerServiceRolePolicy

描述：Amazon CodeGuru Reviewer 代表您存取資源所需的服務連結角色。

AmazonCodeGuruReviewerServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 12 月 3 日 05：31 UTC
- 編輯時間：2020 年 11 月 27 日 15：09 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeGuruSecurityFullAccess

描述：提供 Amazon CodeGuru Security 的完整存取權。

`AmazonCodeGuruSecurityFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonCodeGuruSecurityFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 5 月 9 日，UTC 21：03
- 編輯時間：2023 年 5 月 9 日，UTC 21：03
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCodeGuruSecurityScanAccess

描述：提供使用 Amazon CodeGuru Security 掃描所需的存取權。

AmazonCodeGuruSecurityScanAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonCodeGuruSecurityScanAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 5 月 9 日 20：54 UTC
- 編輯時間：2023 年 5 月 9 日 20：54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCognitoDeveloperAuthenticatedIdentities

描述：提供 Amazon Cognito APIs存取權，以支援來自身分驗證後端的開發人員驗證身分。

`AmazonCognitoDeveloperAuthenticatedIdentities` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCognitoDeveloperAuthenticatedIdentities` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 3 月 24 日 17：22 UTC
- 編輯時間：2015 年 3 月 24 日 17：22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonCognitoIdpEmailServiceRolePolicy

描述：允許 Amazon Cognito 使用者集區服務使用您的 SES 身分傳送電子郵件

AmazonCognitoIdpEmailServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- **建立時間**：2019 年 3 月 21 日 21：32 UTC
- **編輯時間**：2019 年 3 月 21 日，UTC 21：32
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCognitoIdpServiceRolePolicy

描述：允許存取 AWS 服務 Amazon Cognito 使用者集區使用或管理的資源

AmazonCognitoIdpServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 6 月 26 日 22：30 UTC
- 編輯時間：2020 年 6 月 26 日 22：30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonCognitoPowerUser

描述：提供現有 Amazon Cognito 資源的管理存取權。您需要 AWS 帳戶 管理員權限才能建立新的 Cognito 資源。

`AmazonCognitoPowerUser` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCognitoPowerUser` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 3 月 24 日 17：14 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "sms-voice:DescribeAccountAttributes"
      ],
      "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*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCognitoReadOnly

描述：提供 Amazon Cognito 資源的唯讀存取權。

AmazonCognitoReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonCognitoReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 3 月 24 日 17：06 UTC
- 編輯時間：2019 年 8 月 1 日 19：21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoReadOnly

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCognitoUnAuthedIdentitiesSessionPolicy

描述：此政策定義 Cognito 身分集區的未驗證身分允許的一組許可。此政策不適用於做為獨立的許可政策。其做為針對身分集區中角色連接的過度寬鬆政策的護欄。請勿將此政策連接至任何角色，因為 Cognito Identity Service 會在建立登入資料時自動將其納入為縮小範圍的政策。暫時透過增強型流程存取其他 AWS 資源的權限現在將由與服務所提供未經驗證使用者身分相關聯的角色交集，以及此受管政策中由 Cognito 擁有的權限定義。

`AmazonCognitoUnAuthedIdentitiesSessionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonCognitoUnAuthedIdentitiesSessionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 7 月 19 日 23：04 UTC
- 編輯時間：2024 年 11 月 1 日 18：12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
        "polly:*",
        "comprehend:*",
        "translate:*",
        "transcribe:*",
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*",
        "geo:GetMap*",
        "geo:SearchPlaceIndex*",
        "geo:GetPlace",
        "geo:CalculateRoute*",
        "geo:*Geofence",
        "geo:*Geofences",
        "geo:*DevicePosition*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyPair",
        "kms:GenerateDataKeyPairWithoutPlaintext",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonCognitoUnauthenticatedIdentities

描述：此政策定義 Cognito 身分集區的未驗證身分允許的一組許可。這不需要連接到您的不驗證角色，因為 Cognito Identity Service 會在建立登入資料時自動將其納入為範圍縮減政策。暫時透過增強型

流程存取其他 AWS 資源的權限現在將由與服務所提供未經驗證使用者身分相關聯的角色交集，以及 Cognito 所擁有此受管政策中授予的權限定義。

AmazonCognitoUnauthenticatedIdentities 是 AWS 受管政策。

使用此政策

您可以將 AmazonCognitoUnauthenticatedIdentities 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 2 月 1 日 22：36 UTC
- 編輯時間：2023 年 2 月 1 日 22：36 UTC
- ARN: arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonConnect_FullAccess

描述：此政策的目的是授予使用 AWS Connect 資源所需的 Connect 使用者許可。此政策透過 AWS Connect 主控台和公有 APIs提供 Connect 資源的完整存取權

`AmazonConnect_FullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonConnect_FullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 11 月 20 日 19：54 UTC
- 編輯時間：2023 年 3 月 7 日 14：49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonConnectCampaignsServiceLinkedRolePolicy

描述：Amazon Connect Campaigns 服務連結角色的政策

AmazonConnectCampaignsServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 9 月 23 日，UTC 20：54
- 編輯時間：2024 年 10 月 3 日 20：20 UTC

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

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConnectCampaignAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:BatchPutContact",
        "connect:StopContact",
        "connect:DescribeContactFlow",
        "connect:SendOutboundEmail"
      ],
      "Resource" : "arn:aws:connect:*:*:instance/*"
    },
    {
      "Sid" : "EventBridgeListRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EventBridgeManagedResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "connect-campaigns.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTargetsByRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectCampaignsEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:GetMessageTemplate",
        "wisdom:RenderMessageTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectCampaignsEnabled" : "True"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonConnectReadOnlyAccess

描述：准許檢視 中的 Amazon Connect 執行個體 AWS 帳戶。

`AmazonConnectReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonConnectReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 10 月 17 日，UTC 21：00
- 編輯時間：2024 年 6 月 19 日 15：15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonConnectServiceLinkedRolePolicy

描述：允許 Amazon Connect 代表您建立和管理 AWS 資源。

AmazonConnectServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 9 月 7 日 00：21 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

政策版本

政策版本： v53 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "profile:GetIntegration",
        "profile:PutIntegration",
        "profile:DeleteIntegration",
        "profile:ListEventTriggers",
        "profile:ListSegmentDefinitions",
        "profile:ListProfileAttributeValues",
        "profile:CreateSegmentEstimate",
        "profile:GetSegmentEstimate",
        "profile:BatchGetProfile",
        "profile:BatchGetCalculatedAttributeForProfile",
        "profile:GetSegmentMembership",
        "profile:ListDomainLayouts",
        "profile:CreateUploadJob",
        "profile:ListUploadJobs",
        "profile:DetectProfileObjectType",
        "profile:GetSimilarProfiles",
        "profile:GetUploadJob",
        "profile:GetUploadJobPath",
        "profile:StartUploadJob",
        "profile:StopUploadJob",
        "profile:GetProfileRecommendations",
        "profile:GetProfileInsights",
        "profile:ListRecommenders"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
```

```
    },
    {
      "Sid" : "AllowCustomerProfilesEventTriggerForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateEventTrigger",
        "profile:GetEventTrigger",
        "profile:UpdateEventTrigger",
        "profile:DeleteEventTrigger"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/event-triggers/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesDomainLayoutsForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateDomainLayout",
        "profile:UpdateDomainLayout",
        "profile:DeleteDomainLayout",
        "profile:GetDomainLayout"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/layouts/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesSegmentationImportForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetUploadJob",
        "profile:GetUploadJobPath",
        "profile:StartUploadJob",
        "profile:StopUploadJob"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/upload-jobs/*"
      ]
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfileObjects",
      "Effect" : "Allow",
      "Action" : [
```

```
        "profile:ListProfileObjects",
        "profile:GetProfileObjectType",
        "profile:ListObjectTypeAttributes",
        "profile:ListObjectTypeAttributeValues"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfilePredictiveInsights",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetRecommender",
        "profile:CreateRecommender",
        "profile:UpdateRecommender",
        "profile:DeleteRecommender",
        "profile:StopRecommender",
        "profile:StartRecommender"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/recommenders/*"
      ]
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfilesPersonalizeForRecommenderRecipes",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListRecommenderRecipes"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:*"
      ]
    },
    {
      "Sid" : "AllowListIntegrationForCustomerProfile",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListAccountIntegrations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadForCustomerProfileObjectTemplates",
```

```
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjectTypeTemplates",
        "profile:GetProfileObjectTypeTemplate"
      ],
      "Resource" : "arn:aws:profile:*:*:/templates*"
    },
    {
      "Sid" : "AllowAppIntegrationsForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "app-integrations:GetDataIntegration",
        "app-integrations:ListDataIntegrationAssociations",
        "app-integrations:CreateDataIntegrationSchedule",
        "app-integrations:StartDataIntegrationExecution",
        "app-integrations:ListDataIntegrationExecutions",
        "app-integrations:GetDataIntegrationExecution",
        "app-integrations:ListDataIntegrationSchedules",
        "app-integrations:UpdateDataIntegrationSchedule",
        "app-integrations:GetDataIntegrationSchedule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:CreateContent",
        "wisdom:DeleteContent",
        "wisdom:CreateKnowledgeBase",
        "wisdom:GetAssistant",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetContent",
        "wisdom:GetRecommendations",
        "wisdom:GetSession",
        "wisdom:NotifyRecommendationsReceived",
        "wisdom:QueryAssistant",
        "wisdom:StartContentUpload",
        "wisdom:UpdateContent",
```

```
            "wisdom:UntagResource",
            "wisdom:TagResource",
            "wisdom:CreateSession",
            "wisdom:CreateQuickResponse",
            "wisdom:GetQuickResponse",
            "wisdom:SearchQuickResponses",
            "wisdom:StartImportJob",
            "wisdom:GetImportJob",
            "wisdom:ListImportJobs",
            "wisdom:ListQuickResponses",
            "wisdom:UpdateQuickResponse",
            "wisdom:DeleteQuickResponse",
            "wisdom:PutFeedback",
            "wisdom:ListContentAssociations",
            "wisdom:CreateMessageTemplate",
            "wisdom:UpdateMessageTemplate",
            "wisdom:UpdateMessageTemplateMetadata",
            "wisdom:GetMessageTemplate",
            "wisdom:DeleteMessageTemplate",
            "wisdom:ListMessageTemplates",
            "wisdom:SearchMessageTemplates",
            "wisdom:ActivateMessageTemplate",
            "wisdom:DeactivateMessageTemplate",
            "wisdom:CreateMessageTemplateVersion",
            "wisdom:ListMessageTemplateVersions",
            "wisdom:CreateMessageTemplateAttachment",
            "wisdom:DeleteMessageTemplateAttachment",
            "wisdom:RenderMessageTemplate",
            "wisdom:CreateAIAgent",
            "wisdom:CreateAIAgentVersion",
            "wisdom:DeleteAIAgent",
            "wisdom:DeleteAIAgentVersion",
            "wisdom:UpdateAIAgent",
            "wisdom:UpdateAssistantAIAgent",
            "wisdom:RemoveAssistantAIAgent",
            "wisdom:GetAIAgent",
            "wisdom:ListAIAgents",
            "wisdom:ListAIAgentVersions",
            "wisdom:CreateAIPrompt",
            "wisdom:CreateAIPromptVersion",
            "wisdom:DeleteAIPrompt",
            "wisdom:DeleteAIPromptVersion",
            "wisdom:UpdateAIPrompt",
            "wisdom:GetAIPrompt",
```

```
        "wisdom:ListAIPrompts",
        "wisdom:ListAIPromptVersions",
        "wisdom:CreateAIGuardrail",
        "wisdom:CreateAIGuardrailVersion",
        "wisdom:DeleteAIGuardrail",
        "wisdom:DeleteAIGuardrailVersion",
        "wisdom:UpdateAIGuardrail",
        "wisdom:GetAIGuardrail",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:CreateAssistant",
        "wisdom:ListTagsForResource",
        "wisdom:SendMessage",
        "wisdom:GetNextMessage",
        "wisdom:ListMessages",
        "wisdom:Retrieve",
        "wisdom:ListAssistantAssociations"
      ],
      "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" : "AllowCustomerProfilesSegmentationForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateSegmentDefinition",
        "profile:GetSegmentDefinition",
        "profile:DeleteSegmentDefinition",
        "profile:CreateSegmentSnapshot",
        "profile:GetSegmentSnapshot"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/segment-definitions/*"
      ]
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowCognitoForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:ListUserPoolClients"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowWritePermissionForCustomerProfileObjects",
      "Effect" : "Allow",
      "Action" : [
        "profile:PutProfileObject"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorGetOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorListOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:ListVoiceConnectors"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionsForManagingReceiptRules",
      "Effect" : "Allow",
      "Action" : [
        "ses:DescribeReceiptRule",
        "ses:UpdateReceiptRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionForManagingConnectProvidedSESIdentity",
      "Effect" : "Allow",
      "Action" : [
        "ses:DeleteEmailIdentity"
      ],
      "Resource" : "arn:aws:ses:*:*:identity/*.email.connect.aws*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESConfigurationSetPermissionsForSendingEmail",
      "Effect" : "Allow",
      "Action" : [
        "ses:SendRawEmail"
      ],
      "Resource" : "arn:aws:ses:*:*:configuration-set/configuration-set-for-connect-DO-
NOT-DELETE",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "PassRoleToSESForReceiptRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonConnectEmailSESAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ses.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSocialMessagingOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:SendWhatsAppMessage",
        "social-messaging:PostWhatsAppMessageMedia",
        "social-messaging:GetWhatsAppMessageMedia",
        "social-messaging:GetLinkedWhatsAppBusinessAccountPhoneNumber"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWabas",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:ListLinkedWhatsAppBusinessAccounts"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWhatsAppTemplates",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:GetWhatsAppMessageTemplate",
        "social-messaging:ListWhatsAppMessageTemplates"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:waba/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMobileTargetingOperationsForConnect",
      "Effect" : "Allow",
      "Action" : "mobiletargeting:SendMessages",
      "Resource" : "arn:aws:mobiletargeting:*:*:apps/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPollyActions",
      "Effect" : "Allow",
      "Action" : [
        "polly:ListLexicons",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonConnectSynchronizationServiceRolePolicy

描述：允許 Amazon Connect 代表您跨區域同步 AWS 資源。

AmazonConnectSynchronizationServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 10 月 27 日 22：38 UTC
- 編輯時間：2025 年 11 月 21 日 20：19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:Create*",
        "connect:BatchCreate*",
        "connect:Update*",
        "connect:BatchUpdate*",
        "connect:Delete*",
        "connect:BatchDelete*",
        "connect:Describe*",
        "connect:BatchDescribe*",
        "connect:List*",
        "connect:Search*",
        "connect:Associate*",
        "connect:Disassociate*",
        "connect:Get*",
        "connect:BatchGet*",
        "connect:Import*",
        "connect:TagResource",
        "connect:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DisallowedConnectActions",
      "Effect" : "Deny",
      "Action" : [
        "connect:Start*",
        "connect:Stop*",
        "connect:Resume*",
        "connect:Suspend*",
        "connect:*Contact",
        "connect:SearchContacts",
        "connect:*ContactAttributes*",
        "connect:*RealtimeContact*",
        "connect:*AnalyticsData*",
        "connect:*MetricData*",
        "connect:*UserData*",
        "connect:*ContactEvaluation",
        "connect:*AttachedFile*",
        "connect:UpdateContactSchedule",
        "connect:UpdateContactRoutingData",
        "connect:ListContactReferences",
```

```
        "connect:CreateParticipant",
        "connect:CreatePersistentContactAssociation",
        "connect:CreateInstance",
        "connect:DeleteInstance",
        "connect:ListInstances",
        "connect:ReplicateInstance",
        "connect:GetFederationToken",
        "connect:ClaimPhoneNumber",
        "connect:ImportPhoneNumber",
        "connect:ReleasePhoneNumber",
        "connect:SearchAvailablePhoneNumbers",
        "connect:CreateTrafficDistributionGroup",
        "connect:DeleteTrafficDistributionGroup",
        "connect:GetTrafficDistribution",
        "connect:UpdateTrafficDistribution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonConnectVoiceIDFullAccess

描述：提供 Amazon Connect Voice ID 的完整存取權

AmazonConnectVoiceIDFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonConnectVoiceIDFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 9 月 26 日 19：04 UTC
- 編輯時間：2021 年 9 月 26 日 19：04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneBedrockModelConsumptionPolicy

描述：提供使用 Amazon Bedrock 模型的許可，包括叫用針對特定 Amazon DataZone 網域建立的 Amazon Bedrock 應用程式推論設定檔。

AmazonDataZoneBedrockModelConsumptionPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneBedrockModelConsumptionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2024 年 11 月 12 日 22：15 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelConsumptionPolicy

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InvokeDomainInferenceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "ListFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockCreateSessionWithTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateSession",
        "bedrock:TagResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:RequestTag/AmazonDataZoneDomain" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetSession",
        "bedrock:UpdateSession",
        "bedrock:DeleteSession",
        "bedrock:EndSession",
        "bedrock:CreateInvocation",
        "bedrock:ListInvocations",
        "bedrock:PutInvocationStep",
        "bedrock:GetInvocationStep",
        "bedrock:ListInvocationSteps",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockListSessionsPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListSessions",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDataZoneBedrockModelManagementPolicy

描述：提供管理 Amazon Bedrock 模型存取的許可，包括建立、標記和刪除應用程式推論設定檔。

AmazonDataZoneBedrockModelManagementPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneBedrockModelManagementPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2024 年 11 月 12 日 22：14 UTC
- 編輯時間：2024 年 11 月 12 日 22：14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelManagementPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "ManageApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingFoundationModels",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDataZoneDomainExecutionRolePolicy

描述：Amazon DataZone DomainExecutionRole 服務角色的預設政策。Amazon DataZone 使用此角色來編目、探索、管理、共用和分析 Amazon DataZone 網域中的資料。

`AmazonDataZoneDomainExecutionRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneDomainExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 9 月 27 日，UTC 21：55
- 編輯時間：2026 年 2 月 26 日 00：12 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
```

```
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
```

```
            "datazone:GetEnvironmentActionLink",
            "datazone:GetEnvironmentBlueprint",
            "datazone:GetEnvironmentBlueprintConfiguration",
            "datazone:GetEnvironmentCredentials",
            "datazone:GetEnvironmentProfile",
            "datazone:GetFormType",
            "datazone:GetGlossary",
            "datazone:GetGlossaryTerm",
            "datazone:GetGroupProfile",
            "datazone:GetLineageNode",
            "datazone:GetListing",
            "datazone:GetMetadataGenerationRun",
            "datazone:GetProject",
            "datazone:GetRule",
            "datazone:GetSubscription",
            "datazone:GetSubscriptionEligibility",
            "datazone:GetSubscriptionGrant",
            "datazone:GetSubscriptionRequestDetails",
            "datazone:GetSubscriptionTarget",
            "datazone:GetTimeSeriesDataPoint",
            "datazone:GetUserProfile",
            "datazone:ListAccountEnvironments",
            "datazone:ListAssetFilters",
            "datazone:ListAssetRevisions",
            "datazone:ListDataProductRevisions",
            "datazone:ListDataSourceRunActivities",
            "datazone:ListDataSourceRuns",
            "datazone:ListDataSources",
            "datazone:ListDomainUnitsForParent",
            "datazone:ListEntityOwners",
            "datazone:ListEnvironmentActions",
            "datazone:ListEnvironmentBlueprintConfigurationSummaries",
            "datazone:ListEnvironmentBlueprintConfigurations",
            "datazone:ListEnvironmentBlueprints",
            "datazone:ListEnvironmentProfiles",
            "datazone:ListEnvironments",
            "datazone:ListGroupsForUser",
            "datazone:ListLineageNodeHistory",
            "datazone:ListMetadataGenerationRuns",
            "datazone:ListNotifications",
            "datazone:ListPolicyGrants",
            "datazone:ListProjectMemberships",
            "datazone:ListProjects",
            "datazone:ListRules",
```

```
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:QueryGraph",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneEnvironmentRolePermissionsBoundary

描述：Amazon DataZone 會為環境建立 IAM 角色來執行資料分析動作，並在建立這些角色時使用此政策來定義其許可界限。

`AmazonDataZoneEnvironmentRolePermissionsBoundary` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDataZoneEnvironmentRolePermissionsBoundary` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 9 月 11 日 23：38 UTC
- 編輯時間：2023 年 11 月 17 日 23：29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

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

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

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

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

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

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

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

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

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

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneFullAccess

描述：透過 提供 Amazon DataZone 的完整存取權 AWS 管理主控台 ，以及對 所需的相關服務的有限存取權。

AmazonDataZoneFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 9 月 22 日 20：06 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullAccess

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies"
      ],
      "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*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "genai-studio-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
```

```
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneFullUserAccess

描述：提供 Amazon DataZone 的完整存取權，但不允許管理網域、使用者或關聯帳戶。

AmazonDataZoneFullUserAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneFullUserAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 9 月 22 日 21：06 UTC
- 編輯時間：2024 年 11 月 19 日 21：38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
```

```
            "datazone:CreateGlossary",
            "datazone:CreateGlossaryTerm",
            "datazone:CreateListingChangeSet",
            "datazone:CreateProject",
            "datazone:CreateProjectMembership",
            "datazone:CreateRule",
            "datazone:CreateSubscriptionGrant",
            "datazone:CreateSubscriptionRequest",
            "datazone:DeleteAsset",
            "datazone:DeleteAssetFilter",
            "datazone:DeleteAssetType",
            "datazone:DeleteDataProduct",
            "datazone:DeleteDataSource",
            "datazone:DeleteDomainUnit",
            "datazone:DeleteEnvironment",
            "datazone:DeleteEnvironmentBlueprint",
            "datazone:DeleteEnvironmentProfile",
            "datazone:DeleteFormType",
            "datazone:DeleteGlossary",
            "datazone:DeleteGlossaryTerm",
            "datazone:DeleteListing",
            "datazone:DeleteProject",
            "datazone:DeleteProjectMembership",
            "datazone:DeleteRule",
            "datazone:DeleteSubscriptionGrant",
            "datazone:DeleteSubscriptionRequest",
            "datazone:DeleteSubscriptionTarget",
            "datazone:DeleteTimeSeriesDataPoints",
            "datazone:GetAsset",
            "datazone:GetAssetFilter",
            "datazone:GetAssetType",
            "datazone:GetDataProduct",
            "datazone:GetDataSource",
            "datazone:GetDataSourceRun",
            "datazone:GetDomain",
            "datazone:GetDomainUnit",
            "datazone:GetEnvironment",
            "datazone:GetEnvironmentActionLink",
            "datazone:GetEnvironmentBlueprint",
            "datazone:GetEnvironmentCredentials",
            "datazone:GetEnvironmentProfile",
            "datazone:GetFormType",
            "datazone:GetGlossary",
            "datazone:GetGlossaryTerm",
```

```
        "datazone:GetGroupProfile",
        "datazone:GetIamPortalLoginUrl",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:PostTimeSeriesDataPoints",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
```

```
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareOperations",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDataZoneGlueManageAccessRolePolicy

描述：政策授予許可，以允許 Amazon DataZone 啟用資料的發佈和存取授予。

AmazonDataZoneGlueManageAccessRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneGlueManageAccessRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 9 月 22 日 20：21 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy

政策版本

政策版本： v18 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueTagDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLikeIfExists" : {
          "aws:TagKeys" : "DataZoneDiscoverable_*"
        }
      }
    },
    {
      "Sid" : "GlueDataQuality",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListDataQualityResults",
        "glue:GetDataQualityResult"
      ],
      "Resource" : "arn:aws:glue:*:*:dataQualityRuleset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCrawler",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnection",
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "GlueTableDatabaseCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:CreateCatalog",
        "glue:CreateDatabase",
        "glue:DeleteCatalog",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGetTags",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:UpdateDataCellsFilter",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LakeformationResourceFederatedSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "lakeformation:GlueARN" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
```

```
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShares",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/datazone:projectId" : "proj-all"
        }
      }
    },
    {
      "Sid" : "GetRoleForDataZone",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
```

```
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*"
      ]
    },
    {
      "Sid" : "PassRoleForDataLocationRegistration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/datazone_usr_role*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCatalogEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateCatalogS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
```

```
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZonePortalFullAccessPolicy

描述：提供 Amazon DataZone APIs 的完整存取權

`AmazonDataZonePortalFullAccessPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDataZonePortalFullAccessPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 3 月 26 日 18：24 UTC
- 編輯時間：2023 年 3 月 26 日 18：24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZonePreviewConsoleFullAccess

描述：透過 提供 Amazon DataZone 預覽版本的完整存取權 AWS 管理主控台。也提供其他相關服務的選取存取權。

AmazonDataZonePreviewConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZonePreviewConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 3 月 28 日 15：16 UTC
- 編輯時間：2023 年 7 月 13 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneProjectDeploymentPermissionsBoundary

描述：Amazon DataZone 會建立用於部署資料分析專案的 IAM 角色。DataZone 會在建立這些角色時使用此政策來定義其許可的界限。

`AmazonDataZoneProjectDeploymentPermissionsBoundary` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDataZoneProjectDeploymentPermissionsBoundary` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 3 月 21 日 02：54 UTC
- 編輯時間：2023 年 4 月 4 日 02：48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneProjectRolePermissionsBoundary

描述：Amazon DataZone 會為專案建立 IAM 角色以執行資料分析動作，並在建立這些角色時使用此政策來定義其許可界限。

AmazonDataZoneProjectRolePermissionsBoundary 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneProjectRolePermissionsBoundary 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 3 月 21 日 02：51 UTC
- 編輯時間：2023 年 3 月 21 日 02：51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneRedshiftGlueProvisioningPolicy

描述：Amazon DataZone 是一種資料管理服務，可讓您編目、探索、控管、共用和分析您的資料。使用 Amazon DataZone，您可以跨帳戶和支援的區域共用和存取您的資料。Amazon DataZone 可簡化跨 AWS 服務的體驗，包括但不限於 Amazon Redshift、Amazon Athena、 AWS Glue 和 AWS Lake Formation。

`AmazonDataZoneRedshiftGlueProvisioningPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDataZoneRedshiftGlueProvisioningPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 9 月 22 日 20：19 UTC
- 編輯時間：2024 年 10 月 23 日 18：29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "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",
        "iam:DeletePolicyVersion"
      ],
      "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*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneRedshiftManageAccessRolePolicy

描述：此政策提供 Amazon DataZone 將 Amazon Redshift 資料發佈至目錄的許可。它還授予 Amazon DataZone 許可，以授予對 目錄中 Amazon Redshift 或 Amazon Redshift Serverless 發佈資產的存取權或撤銷存取權。

AmazonDataZoneRedshiftManageAccessRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneRedshiftManageAccessRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 9 月 22 日 20：15 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "createAndDeleteWorkgroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "getNamespacePermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetNamespace",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:DeleteNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "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*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

描述：AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 政策是在 Amazon DataZone 佈建的 SageMaker 環境中建立的執行角色上允許的許可清單。

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 4 月 23 日，UTC 23：01
- 編輯時間：2026 年 3 月 11 日 21：12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
```

```
      ]
    },
    {
      "Sid" : "AllowSageMakerProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile",
        "sagemaker:UpdateUserProfile",
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:*/*"
    },
    {
      "Sid" : "AllowLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsForDomainResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateApp",
            "CreateSpace",
            "CreateUserProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStudioActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListSpaces",
        "sagemaker:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
```

```
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*",
        "datazone:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
```

```
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "groundtruthlabeling:*",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowRAMInvitation",
      "Effect" : "Allow",
      "Action" : "ram:AcceptResourceShareInvitation",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "dzd*"
        }
      }
    },
```

```
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker*",
        "arn:aws:ecr:*:*:repository/datazone*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
```

```
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
```

```
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
```

```
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "states.amazonaws.com",
            "lakeformation.amazonaws.com",
            "events.amazonaws.com",
            "sagemaker.amazonaws.com",
            "forecast.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
```

```
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
```

```
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:domain/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:ListJobs",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
```

```
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:GetTable",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:ListSchemas",
        "glue:BatchGetJobs",
        "glue:GetConnection",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueActionsWithEnvironmentTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
```

```
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:ListSchemas",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGlueDefaultAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:RunStatement"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
```

```
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:connection/dz-sm-*",
        "arn:aws:glue:*:*:session/*"
      ]
    },
    {
      "Sid" : "AllowRedshiftClusterActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowCreateClusterUser",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterUser"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*"
      ]
    },
    {
      "Sid" : "AllowCreateSecretActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*",
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
```

```
          "aws:RequestTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
```

```
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventBridgeRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEMR",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSOAction",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyNotAction",
      "Effect" : "Deny",
      "NotAction" : [
        "sagemaker:*",
        "sagemaker-geospatial:*",
        "sqlworkbench:*",
        "datazone:*",
        "forecast:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
```

```
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
```

```
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
```

```
            "ecr:DeleteRepository",
            "ecr:PutImage",
            "ecr:StartImageScan",
            "ecr:TagResource",
            "ecr:UntagResource",
            "elasticfilesystem:DescribeFileSystems",
            "elasticfilesystem:DescribeMountTargets",
            "elasticmapreduce:DescribeCluster",
            "elasticmapreduce:ListInstanceGroups",
            "elasticmapreduce:ListClusters",
            "events:PutRule",
            "events:DescribeRule",
            "events:PutTargets",
            "events:TagResource",
            "events:ListTagsForResource",
            "fsx:DescribeFileSystems",
            "glue:SearchTables",
            "glue:NotifyEvent",
            "glue:StartBlueprintRun",
            "glue:PutWorkflowRunProperties",
            "glue:StopCrawler",
            "glue:DeleteJob",
            "glue:DeleteWorkflow",
            "glue:UpdateCrawler",
            "glue:DeleteBlueprint",
            "glue:UpdateWorkflow",
            "glue:StartCrawler",
            "glue:ResetJobBookmark",
            "glue:UpdateJob",
            "glue:StartWorkflowRun",
            "glue:StopCrawlerSchedule",
            "glue:ResumeWorkflowRun",
            "glue:DeleteCrawler",
            "glue:UpdateBlueprint",
            "glue:BatchStopJobRun",
            "glue:StopWorkflowRun",
            "glue:BatchGet*",
            "glue:UpdateCrawlerSchedule",
            "glue:DeleteConnection",
            "glue:UpdateConnection",
            "glue:Get*",
            "glue:BatchDeleteConnection",
            "glue:StartCrawlerSchedule",
            "glue:StartJobRun",
```

```
            "glue:CreateWorkflow",
            "glue:*DataQuality*",
            "glue:List*",
            "glue:CreateSession",
            "glue:RunStatement",
            "glue:BatchCreatePartition",
            "glue:CreateDatabase",
            "glue:CreatePartitionIndex",
            "glue:CreateTable",
            "glue:BatchUpdatePartition",
            "glue:BatchDeletePartition",
            "glue:UpdateTable",
            "glue:DeleteTableVersion",
            "glue:DeleteTable",
            "glue:DeleteColumnStatisticsForPartition",
            "glue:DeleteColumnStatisticsForTable",
            "glue:DeletePartitionIndex",
            "glue:UpdateColumnStatisticsForPartition",
            "glue:UpdateColumnStatisticsForTable",
            "glue:BatchDeleteTableVersion",
            "glue:BatchDeleteTable",
            "glue:CreatePartition",
            "glue:DeletePartition",
            "glue:UpdatePartition",
            "glue:CreateBlueprint",
            "glue:CreateJob",
            "glue:CreateConnection",
            "glue:CreateCrawler",
            "groundtruthlabeling:*",
            "iam:CreateServiceLinkedRole",
            "iam:GetRole",
            "iam:ListRoles",
            "iam:PassRole",
            "kms:DescribeKey",
            "kms:ListAliases",
            "kms:Decrypt",
            "kms:ListKeys",
            "kms:Encrypt",
            "kms:GenerateDataKey",
            "kms:RetireGrant",
            "lakeformation:GetDataAccess",
            "lambda:ListFunctions",
            "lambda:InvokeFunction",
            "logs:CreateLogDelivery",
```

```
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:DeleteLogDelivery",
            "logs:Describe*",
            "logs:GetLogDelivery",
            "logs:GetLogEvents",
            "logs:ListLogDeliveries",
            "logs:PutLogEvents",
            "logs:UpdateLogDelivery",
            "ram:AcceptResourceShareInvitation",
            "rds:DescribeDBInstances",
            "redshift:CreateClusterUser",
            "redshift:GetClusterCredentials",
            "redshift:GetClusterCredentialsWithIAM",
            "redshift:DescribeClusters",
            "redshift-data:BatchExecuteStatement",
            "redshift-data:CancelStatement",
            "redshift-data:DescribeStatement",
            "redshift-data:DescribeTable",
            "redshift-data:ExecuteStatement",
            "redshift-data:GetStatementResult",
            "redshift-data:ListSchemas",
            "redshift-data:ListTables",
            "redshift-serverless:ListNamespaces",
            "redshift-serverless:ListWorkgroups",
            "redshift-serverless:GetNamespace",
            "redshift-serverless:GetWorkgroup",
            "redshift-serverless:GetCredentials",
            "s3:GetBucketAcl",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject",
            "s3:AbortMultipartUpload",
            "s3:CreateBucket",
            "s3:GetBucketLocation",
            "s3:ListBucket",
            "s3:ListAllMyBuckets",
            "s3:GetBucketCors",
            "s3:PutBucketCors",
            "s3:DeleteObjectVersion",
            "s3:PutObjectRetention",
            "s3:ReplicateObject",
            "s3:RestoreObject",
```

```
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:TagResource",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine",
        "tag:GetResources",
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyUpdateNotebookInstanceLifecycleConfig",
      "Effect" : "Deny",
      "Action" : [
        "sagemaker:UpdateNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneSageMakerManageAccessRolePolicy

描述：AmazonDataZoneSageMakerManageAccessRolePolicy 政策授予 Amazon DataZone 許可，以授予使用者對 SageMaker 環境中各種資源的存取權。

AmazonDataZoneSageMakerManageAccessRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonDataZoneSageMakerManageAccessRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 4 月 23 日，UTC 23：34
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:ListTags",
        "sagemaker:DescribeDomain",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelPackageGroupPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:DeleteModelPackageGroupPolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerRAMResourcePolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutResourcePolicy",
        "sagemaker:GetResourcePolicy",
        "sagemaker:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:feature-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMTagResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMDeleteResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "AmazonSageMakerRAMCreateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "sagemaker:*"
          ]
        },
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerS3BucketPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
```

```
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:DeleteRepositoryPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSGrantPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDataZoneSageMakerProvisioningRolePolicy

描述：AmazonDataZoneSageMakerProvisioningRolePolicy 政策會授予 Amazon DataZone 與 Amazon SageMaker 交互操作所需的許可。

`AmazonDataZoneSageMakerProvisioningRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDataZoneSageMakerProvisioningRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- **類型**： AWS 受管政策
- **建立時間**：2024 年 4 月 23 日，UTC 23：32
- **編輯時間**：2026 年 2 月 12 日 18：01 UTC

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

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false",
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "DeleteSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ],
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageEnvironmentRole",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "sagemaker:ListDomains"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSKeyValidation",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection",
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDetectiveFullAccess

描述：提供 Amazon Detective 服務的完整存取權，以及主控台 UI 相依性的範圍存取權

AmazonDetectiveFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDetectiveFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 4 月 30 日 17：57 UTC
- 編輯時間：2023 年 5 月 17 日 19：39 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveFullAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDetectiveInvestigatorAccess

描述：提供 Amazon Detective 服務的調查人員存取權，以及主控台 UI 相依性的範圍存取權。此政策授予深入 Detective 的許可，以用於調查目的和對 Guardduty 的有限寫入存取。

`AmazonDetectiveInvestigatorAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonDetectiveInvestigatorAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 1 月 17 日 15：24 UTC
- 編輯時間：2023 年 11 月 27 日 03：13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDetectiveMemberAccess

描述：提供 Amazon Detective 服務的成員存取權，以及主控台 UI 相依性的範圍存取權。

AmazonDetectiveMemberAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDetectiveMemberAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 1 月 17 日 15：16 UTC
- 編輯時間：2023 年 1 月 17 日 15：16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDetectiveOrganizationsAccess

描述：提供 Organizations 存取權，以管理 Amazon Detective 的委派管理員，以及主控台 UI 相依性的範圍存取。這也授予為 Detective 建立服務連結角色的許可。

`AmazonDetectiveOrganizationsAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDetectiveOrganizationsAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 3 月 2 日 15：20 UTC

- **編輯時間**：2023 年 3 月 2 日 15：20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDetectiveServiceLinkedRolePolicy

描述：允許 Amazon Detective 代表您進行服務呼叫

AmazonDetectiveServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 18 日 19：47 UTC
- 編輯時間：2021 年 11 月 18 日 19：47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDevOpsGuruConsoleFullAccess

描述：政策會授予 DevOps Guru 主控台的完整存取權。

`AmazonDevOpsGuruConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDevOpsGuruConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 12 月 17 日 18：43 UTC
- 編輯時間：2022 年 8 月 25 日 18：18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDevOpsGuruFullAccess

描述：提供 Amazon DevOps Guru 的完整存取權。

AmazonDevOpsGuruFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDevOpsGuruFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 1 日 16：38 UTC
- 編輯時間：2022 年 8 月 25 日 18：23 UTC

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

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDevOpsGuruOrganizationsAccess

描述：提供在組織內啟用和管理 Amazon DevOps Guru 的存取權。

AmazonDevOpsGuruOrganizationsAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDevOpsGuruOrganizationsAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 15 日 23：50 UTC

- **編輯時間**：2021 年 11 月 15 日 23：50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDevOpsGuruReadOnlyAccess

描述：提供 Amazon DevOps Guru 主控台的唯讀存取權。

AmazonDevOpsGuruReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDevOpsGuruReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 1 日 16：34 UTC
- 編輯時間：2022 年 8 月 25 日 18：11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDevOpsGuruServiceRolePolicy

描述：Amazon DevOpsGuru 存取 資源所需的服務連結角色。

`AmazonDevOpsGuruServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 1 日 10：24 UTC
- 編輯時間：2023 年 1 月 10 日 14：36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonDMSCloudWatchLogsRole

描述：提供將 DMS 複寫日誌上傳至客戶帳戶中 cloudwatch 日誌的存取權。

AmazonDMSCloudWatchLogsRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonDMSCloudWatchLogsRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 1 月 7 日 23：44 UTC
- 編輯時間：2023 年 5 月 23 日，UTC 21：32
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDMSRedshiftS3Role

描述：提供管理 DMS Redshift 端點 S3 設定的存取權。

AmazonDMSRedshiftS3Role 是 AWS 受管政策。

使用此政策

您可以將 AmazonDMSRedshiftS3Role 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 4 月 20 日 17：05 UTC
- 編輯時間：2019 年 7 月 8 日 18：19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role

政策版本

政策版本： v3 （ 預設 ）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDMSVPCManagementRole

描述：提供管理 AWS 受管客戶組態 VPC 設定的存取權

AmazonDMSVPCManagementRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonDMSVPCManagementRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 11 月 18 日 16：33 UTC
- 編輯時間：2024 年 7 月 25 日 15：19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDocDB-ElasticServiceRolePolicy

描述：允許 Amazon DocumentDB-Elastic 代表您管理 AWS 資源。

`AmazonDocDB-ElasticServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 30 日 14：17 UTC
- 編輯時間：2022 年 11 月 30 日 14：17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDocDBConsoleFullAccess

描述：提供使用 以 MongoDB 相容性管理 Amazon DocumentDB 的完整存取權 AWS 管理主控台。MongoDB 請注意，此政策也授予帳戶內所有 SNS 主題發佈的完整存取權、建立和編輯 Amazon EC2 執行個體和 VPC 組態的許可、在 Amazon KMS 上檢視和列出金鑰的許可，以及 Amazon RDS 和 Amazon Neptune 的完整存取權。

AmazonDocDBConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDocDBConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 1 月 9 日 20：37 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbSids",
      "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",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction",
        "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" : [
        "*"
      ]
    },
    {
      "Sid" : "DependencySids",
      "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" : [
        "*"
      ]
    },
    {
      "Sid" : "DocdbSLRSid",
      "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" : "DocdbElasticSLRSid",
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDocDBElasticFullAccess

描述：提供 Amazon DocumentDB Elastic Clusters 的完整存取權，以及其相依性的其他必要許可，包括 EC2、KMS、SecretsManager、CloudWatch 和 IAM。

AmazonDocDBElasticFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDocDBElasticFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 6 月 5 日 13：51 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbElasticSid",
      "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",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Sid",
      "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"
        }
```

```
      }
    },
    {
      "Sid" : "KMSSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ],
          "aws:ResourceTag/DocDBElasticFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "KMSGrantSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/DocDBElasticFullAccess" : "*",
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "SecretManagerSid",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchSid",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SLRSid",
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDocDBElasticReadOnlyAccess

描述：提供 Amazon DocDB-Elastic 和 CloudWatch 指標的唯讀存取權。

`AmazonDocDBElasticReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDocDBElasticReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 6 月 8 日 14：37 UTC
- 編輯時間：2023 年 6 月 21 日 16：57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDocDBFullAccess

描述：提供具有 MongoDB 相容性的 Amazon DocumentDB 完整存取權。 MongoDB 請注意，此政策也授予帳戶內所有 SNS 主題發佈的完整存取權，以及 Amazon RDS 和 Amazon Neptune 的完整存取權。

AmazonDocDBFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDocDBFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 1 月 9 日 20：21 UTC
- 編輯時間：2019 年 1 月 9 日 20：21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
```

```
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDocDBReadOnlyAccess

描述：提供具有 MongoDB 相容性的 Amazon DocumentDB 唯讀存取權。請注意，此政策也會授予 Amazon RDS 和 Amazon Neptune 資源的存取權。

`AmazonDocDBReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDocDBReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 1 月 9 日 20：30 UTC
- 編輯時間：2019 年 1 月 9 日 20：30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDRSVPCManagement

描述：提供管理 Amazon 受管客戶組態 VPC 設定的存取權

AmazonDRSVPCManagement 是 AWS 受管政策。

使用此政策

您可以將 AmazonDRSVPCManagement 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 9 月 2 日 00：09 UTC
- 編輯時間：2015 年 9 月 2 日 00：09 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDRSVPCManagement

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDynamoDBFullAccess

描述：透過 提供 Amazon DynamoDB 的完整存取權 AWS 管理主控台。

AmazonDynamoDBFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonDynamoDBFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2021 年 1 月 29 日 17：38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonDynamoDBFullAccess_v2

描述：提供 Amazon DynamoDB 的完整存取權

AmazonDynamoDBFullAccess_v2 是 AWS 受管政策。

使用此政策

您可以將 AmazonDynamoDBFullAccess_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 5 月 22 日 14：52 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess_v2`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DDBAndDAXFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:*",
        "dax:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaIntegration",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DaxSNSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchMonitoring",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListKinesisResources",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListEC2ResourcesForDaxClusterCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchInsightsRules",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Sid" : "ServiceRoleCreation",
      "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"
          ]
        }
      }
    },
    {
      "Sid" : "IamIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDynamoDBFullAccesswithDataPipeline

描述：此政策位於棄用路徑上。如需指引，請參閱 文件：https：//https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html。透過 提供 Amazon DynamoDB 的完整存取權，包括使用 AWS 資料管道匯出/匯入 AWS 管理主控台。

AmazonDynamoDBFullAccesswithDataPipeline 是 AWS 受管政策。

使用此政策

您可以將 AmazonDynamoDBFullAccesswithDataPipeline 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 11 月 12 日 02：17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonDynamoDBReadOnlyAccess

描述：透過 提供 Amazon DynamoDB 的唯讀存取權 AWS 管理主控台。

`AmazonDynamoDBReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonDynamoDBReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2024 年 11 月 18 日 17：38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:GetAbacStatus",
        "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*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEBSCSIDriverPolicy

描述：IAM 政策，允許 CSI 驅動程式服務帳戶代表您呼叫相關服務，例如 EC2。

AmazonEBSCSIDriverPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEBSCSIDriverPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 4 月 4 日 17：24 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/vol-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:LockSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2ContainerRegistryFullAccess

描述：提供 Amazon ECR 資源的管理存取權

`AmazonEC2ContainerRegistryFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEC2ContainerRegistryFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 12 月 21 日 17：06 UTC
- 編輯時間：2020 年 12 月 5 日 00：04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2ContainerRegistryPowerUser

描述：提供 Amazon EC2 Container Registry 儲存庫的完整存取權，但不允許刪除儲存庫或變更政策。

AmazonEC2ContainerRegistryPowerUser 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2ContainerRegistryPowerUser 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 12 月 21 日 17：05 UTC
- 編輯時間：2019 年 12 月 10 日 20：48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEC2ContainerRegistryPullOnly

描述：提供從 Amazon EC2 Container Registry 儲存庫提取映像的存取權。

AmazonEC2ContainerRegistryPullOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2ContainerRegistryPullOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 10 月 4 日 16：58 UTC

- **編輯時間**：2024 年 10 月 4 日 16：58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchImportUpstreamImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEC2ContainerRegistryReadOnly

描述：提供 Amazon EC2 Container Registry 儲存庫的唯讀存取權。

AmazonEC2ContainerRegistryReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2ContainerRegistryReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 12 月 21 日 17：04 UTC
- 編輯時間：2019 年 12 月 10 日，UTC 20：56
- ARN: arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2ContainerServiceAutoscaleRole

描述：為 Amazon EC2 Container Service 啟用任務自動擴展的政策

`AmazonEC2ContainerServiceAutoscaleRole` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEC2ContainerServiceAutoscaleRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 5 月 12 日 23：25 UTC
- 編輯時間：2018 年 2 月 5 日 19：15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2ContainerServiceEventsRole

描述：為 EC2 Container Service 啟用 CloudWatch Events 的政策

`AmazonEC2ContainerServiceEventsRole` 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2ContainerServiceEventsRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 5 月 30 日 16：51 UTC
- 編輯時間：2023 年 3 月 6 日 22：25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2ContainerServiceforEC2Role

描述：Amazon EC2 Container Service 的 Amazon EC2 角色的預設政策。

`AmazonEC2ContainerServiceforEC2Role` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEC2ContainerServiceforEC2Role` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策

- **建立時間**：2015 年 3 月 19 日 18：45 UTC
- **編輯時間**：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*",
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEC2ContainerServiceRole

描述：Amazon ECS 服務角色的預設政策。

`AmazonEC2ContainerServiceRole` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEC2ContainerServiceRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 4 月 9 日 16：14 UTC
- 編輯時間：2016 年 8 月 11 日 13：08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2FullAccess

描述：透過 提供 Amazon EC2 的完整存取權 AWS 管理主控台。

AmazonEC2FullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2FullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2018 年 11 月 27 日 02：16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2FullAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEC2ImageReferencesAccessPolicy

描述：提供唯讀存取權，以便在使用 DescribeImageReferences 時掃描所有支援的資源類型以取得相關資料。

AmazonEC2ImageReferencesAccessPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2ImageReferencesAccessPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 26 日 19：19 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEC2ImageReferencesAccessPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:DescribeImageReferences",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ssm:DescribeParameters",
        "ssm:GetParameters",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:GetContainerRecipe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ec2-images.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2ReadOnlyAccess

描述：透過 提供 Amazon EC2 的唯讀存取權 AWS 管理主控台。

`AmazonEC2ReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEC2ReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2015 年 2 月 6 日 18：40 UTC
- **編輯時間**：2026 年 2 月 12 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEC2RoleforAWSCodeDeploy

描述：提供 S3 儲存貯體的 EC2 存取權以下載修訂。EC2 執行個體上的 CodeDeploy 代理程式需要此角色。

AmazonEC2RoleforAWSCodeDeploy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2RoleforAWSCodeDeploy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 5 月 19 日 18：10 UTC
- 編輯時間：2017 年 3 月 20 日 17：14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2RoleforAWSCodeDeployLimited

描述：提供對 S3 儲存貯體的 EC2 有限存取權以下載修訂。EC2 執行個體上的 CodeDeploy 代理程式需要此角色。

`AmazonEC2RoleforAWSCodeDeployLimited` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEC2RoleforAWSCodeDeployLimited` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策

- **建立時間**：2020 年 8 月 24 日 17：55 UTC
- **編輯時間**：2022 年 1 月 20 日 21：37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2RoleforDataPipelineRole

描述：資料管道服務角色的 Amazon EC2 角色的預設政策。

AmazonEC2RoleforDataPipelineRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2RoleforDataPipelineRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2016 年 2 月 22 日 17：24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2RoleforSSM

描述：此政策即將棄用。請使用 AmazonSSMManagedInstanceCore 政策在 EC2 執行個體上啟用 AWS Systems Manager 服務核心功能。如需詳細資訊，請參閱 https：//https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html

`AmazonEC2RoleforSSM` 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2RoleforSSM 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 5 月 29 日 17：48 UTC
- 編輯時間：2019 年 1 月 24 日 19：20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2RolePolicyForLaunchWizard

描述：適用於 EC2 的 Amazon LaunchWizard 服務角色的受管政策

AmazonEC2RolePolicyForLaunchWizard 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2RolePolicyForLaunchWizard 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 11 月 13 日 08：05 UTC
- 編輯時間：2024 年 9 月 25 日，UTC 22：40
- ARN: arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackintForAWSBackup"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEC2SpotFleetAutoscaleRole

描述：為 Amazon EC2 Spot Fleet 啟用 Autoscaling 的政策

`AmazonEC2SpotFleetAutoscaleRole` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEC2SpotFleetAutoscaleRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 8 月 19 日 18：27 UTC
- 編輯時間：2019 年 2 月 18 日 19：17 UTC

- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEC2SpotFleetTaggingRole

描述：允許 EC2 Spot Fleet 代表您請求、終止和標記 Spot 執行個體。

AmazonEC2SpotFleetTaggingRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonEC2SpotFleetTaggingRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 6 月 29 日 18：19 UTC
- 編輯時間：2020 年 4 月 23 日 19：30 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonECS_FullAccess

描述：提供 Amazon ECS 資源的管理存取權，並透過存取其他服務 AWS 資源來啟用 ECS 功能，包括 VPCs、Auto Scaling 群組和 CloudFormation 堆疊。

`AmazonECS_FullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonECS_FullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 7 日 21：36 UTC
- 編輯時間：2024 年 8 月 13 日 19：39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

政策版本

政策版本： v21 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSIntegrationsManagementPolicy",
      "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" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
    },
    {
      "Sid" : "ManagedCloudformationResourcesCleanupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteInternetGateway",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
        }
      }
    },
    {
      "Sid" : "TasksPassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "InfrastructurePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInfrastructureRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstancePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AutoScalingPassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsAutoscaleRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ServiceLinkedRoleCreationPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "ecs.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.application-autoscaling.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateTargetGroup",
            "CreateRule",
            "CreateListener",
            "CreateLoadBalancer"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonECSComputeServiceRolePolicy

描述：啟用 Amazon ECS Compute 以管理 EC2 執行個體和相關資源作為 ECS 受管執行個體一部分的政策

AmazonECSComputeServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 3 月 24 日 17：37 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonECSComputeServiceRolePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeFleets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteManagedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TerminateManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonECSInfrastructureRoleforExpressGatewayServices

描述：這些許可可讓 Amazon ECS 自動佈建和管理 Express Gateway Services 所需的基礎設施元件，包括負載平衡、安全群組、SSL 憑證和自動擴展組態。

AmazonECSInfrastructureRoleforExpressGatewayServices 是 AWS 受管政策。

使用此政策

您可以將 AmazonECSInfrastructureRoleforExpressGatewayServices 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 11 月 12 日 20：34 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRoleforExpressGatewayServices

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ServiceLinkedRoleCreateOperations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ecs.application-autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
```

```
        "elasticloadbalancing:DeleteListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateELBResources",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateListener",
            "CreateRule",
            "CreateTargetGroup"
          ]
        }
      }
    },
    {
      "Sid" : "BlanketAllowCreateSecurityGroupsInVPCs",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateSecurityGroupResourcesWithTags",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifySecurityGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateEC2Resources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress",
            "AuthorizeSecurityGroupEgress"
          ]
        }
      }
    },
    {
      "Sid" : "CertificateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate",
        "acm:AddTagsToCertificate",
        "acm:DeleteCertificate",
        "acm:DescribeCertificate"
      ],
      "Resource" : [
        "arn:aws:acm:*:*:certificate/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:TagResource",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "ApplicationAutoscalingPolicyOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "ecs"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ]
    },
    {
      "Sid" : "CloudWatchAlarmCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "CloudWatchAlarmOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsCreateOperations",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonECSInfrastructureRolePolicyForLoadBalancers

描述：提供代表您管理與 ECS 工作負載相關聯之負載平衡器所需的其他 AWS 服務資源的存取權。

AmazonECSInfrastructureRolePolicyForLoadBalancers 是 AWS 受管政策。

使用此政策

您可以將 AmazonECSInfrastructureRolePolicyForLoadBalancers 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 7 月 17 日 16：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForLoadBalancers`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
    },
```

```
    {
      "Sid" : "ALBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*"
      ]
    },
    {
      "Sid" : "NLBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/net/*/*/*"
      ]
    },
    {
      "Sid" : "ALBModifyRules",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyRule",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonECSInfrastructureRolePolicyForManagedInstances

描述：提供 ECS 存取權，以建立和管理 EC2 受管資源

AmazonECSInfrastructureRolePolicyForManagedInstances 是 AWS 受管政策。

使用此政策

您可以將 AmazonECSInfrastructureRolePolicyForManagedInstances 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 9 月 26 日 18：04 UTC
- 編輯時間：2026 年 2 月 26 日 18：27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForManagedInstances

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateLaunchTemplateVersionsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ProvisionEC2InstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateFleetForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
```

```
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "RunInstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForECSManagedLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
```

```
        "arn:aws:ec2:*::image/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "TagOnCreateEC2ResourcesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "CreateLaunchTemplate",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "PassInstanceRoleForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.*"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEC2Spot",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ]
    },
    {
      "Sid" : "DescribeEC2ResourcesManagedByECS",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeCapacityReservations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListResourceGroupResources",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

描述：提供私有憑證授權單位、 AWS Secrets Manager 和其他 AWS 服務 必要的管理存取權，以代表您管理 ECS Service Connect TLS 功能。

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 是 AWS 受管政策。

使用此政策

您可以
將 AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2024 年 1 月 19 日 20：08 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager: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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonECSInfrastructureRolePolicyForVolumes

描述：提供代表您管理與 ECS 工作負載相關聯之磁碟區所需的其他 AWS 服務資源的存取權。

AmazonECSInfrastructureRolePolicyForVolumes 是 AWS 受管政策。

使用此政策

您可以將 AmazonECSInfrastructureRolePolicyForVolumes 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2024 年 1 月 10 日 22：56 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "CreateEBSManagedVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "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" : "DescribeInstancesForAttachingVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
```

```
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonECSInfrastructureRolePolicyForVpcLattice

描述：提供代表您管理 ECS 工作負載中 VPC Lattice 功能所需的其他 AWS 服務資源的存取權。

AmazonECSInfrastructureRolePolicyForVpcLattice 是 AWS 受管政策。

使用此政策

您可以將 AmazonECSInfrastructureRolePolicyForVpcLattice 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 15 日 20：02 UTC

- **編輯時間**：2024 年 11 月 15 日 20：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForVpcLattice`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManagedVpcLatticeTargetRegistration",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:RegisterTargets",
        "vpc-lattice:DeregisterTargets"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "DescribeVpcLatticeTargetGroup",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:GetTargetGroup",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "ListVpcLatticeTargets",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:ListTargets",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
```

```
    },
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonECSInstanceRolePolicyForManagedInstances

描述：Amazon ECS 受管執行個體的 Amazon ECS 執行個體角色的預設政策。

`AmazonECSInstanceRolePolicyForManagedInstances` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonECSInstanceRolePolicyForManagedInstances` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- **建立時間**：2025 年 9 月 26 日，UTC 23：49
- **編輯時間**：2026 年 2 月 12 日 17：58 UTC

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

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAgentDiscoverPollEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DiscoverPollEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSAgentRegisterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterContainerInstance"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    },
    {
      "Sid" : "ECSAgentPollPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll"
      ],
      "Resource" : "arn:aws:ecs:*:*:container-instance/*"
    },
    {
      "Sid" : "ECSAgentTelemetryPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:StartTelemetrySession",
        "ecs:PutSystemLogEvents"
      ],
      "Resource" : "arn:aws:ecs:*:*:container-instance/*"
    },
    {
      "Sid" : "ECSAgentStateChangePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:SubmitAttachmentStateChanges",
        "ecs:SubmitTaskStateChange"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonECSServiceRolePolicy

描述：啟用 Amazon ECS 以管理叢集的政策。

AmazonECSServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 14 日 01：18 UTC

- **編輯時間**：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy

政策版本

政策版本： v23 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:AssociateTrunkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateTrunkInterface",
        "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" : "OpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "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" : "*"
    },
    {
      "Sid" : "CloudMapResourceAttributeManagement",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:UpdateServiceAttributes"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonECSTaskExecutionRolePolicy

描述：提供執行 Amazon ECS 任務所需的其他 AWS 服務資源的存取權

AmazonECSTaskExecutionRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonECSTaskExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 11 月 16 日 18：48 UTC
- 編輯時間：2017 年 11 月 16 日 18：48 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEFSCSIDriverPolicy

描述：提供 EFS 資源的管理存取權和 EC2 的讀取存取權

AmazonEFSCSIDriverPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEFSCSIDriverPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 7 月 25 日 20：10 UTC
- 編輯時間：2023 年 7 月 25 日 20：10 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEKS_CNI_Policy

描述：此政策提供 Amazon VPC CNI 外掛程式 (amazon-vpc-cni-k8s) 修改 EKS 工作者節點上 IP 地址組態所需的許可。此許可集允許 CNI 代表您列出、描述和修改彈性網路界面。如需 AWS VPC CNI 外掛程式的詳細資訊，請參閱：https：//https://github.com/aws/amazon-vpc-cni-k8s

AmazonEKS_CNI_Policy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKS_CNI_Policy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 5 月 27 日，UTC 21：07
- 編輯時間：2026 年 3 月 4 日 19：12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:DescribeSecurityGroups",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSBlockStoragePolicy

描述：連接到 EKS 叢集角色的政策，授予管理叢集區塊儲存資源的許可。

AmazonEKSBlockStoragePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSBlockStoragePolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 10 月 30 日 20：18 UTC
- 編輯時間：2024 年 10 月 30 日 20：18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "kubernetes.io/created-for/*",
            "Name",
            "KubernetesCluster"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
```

```
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeSnapshotName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "Name"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSClusterPolicy

描述：此政策提供 Kubernetes 代表您管理 資源所需的許可。Kubernetes 需要 Ec2：CreateTags 許可，才能在 EC2 資源上放置識別資訊，包括但不限於執行個體、安全群組和彈性網路界面。

AmazonEKSClusterPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSClusterPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 5 月 27 日，UTC 21：06
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSClusterPolicy

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSClusterPolicy",
      "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",
        "ec2:DescribeInstanceTopology",
        "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" : "*"
    },
    {
      "Sid" : "AmazonEKSClusterPolicySLRCreate",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonEKSClusterPolicyENIDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "amazon-vpc-cni"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSComputePolicy

描述：連接到 EKS 叢集角色的政策，授予管理叢集運算資源的許可。

AmazonEKSComputePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSComputePolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 11 月 1 日 21：46 UTC

- **編輯時間**：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSComputePolicy`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-node-class-name" : "*",
          "aws:RequestTag/eks:kubernetes-node-pool-name" : "*"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-node-class-name",
            "eks:kubernetes-node-pool-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
```

```
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSConnectorServiceRolePolicy

描述：此政策允許 Amazon EKS 管理 EKS 連接器 AWS 的資源

AmazonEKSConnectorServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 9 月 4 日，UTC 20：31
- 編輯時間：2025 年 10 月 15 日 22：34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
```

```
        },
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.ssm"
        }
      }
    },
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSDashboardConsoleReadOnly

描述：提供唯讀存取權，以在 Amazon EKS 主控台中檢視儀表板。儀表板會使用 AWS Organizations 彙總多個叢集和相關資源的相關資訊。

`AmazonEKSDashboardConsoleReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSDashboardConsoleReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 6 月 19 日 17：22 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSDashboardConsoleReadOnly

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSDashboardReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListDashboardData",
        "eks:ListDashboardResources",
        "eks:DescribeClusterVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSDashboardServiceRolePolicy

描述：此政策可讓 Amazon EKS 儀表板存取和顯示整個組織的資訊。此政策允許 EKS Dashboard 服務收集有關您的 AWS Organizations 結構和帳戶的資訊。

AmazonEKSDashboardServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 5 月 8 日 19：07 UTC
- 編輯時間：2025 年 5 月 8 日 19：07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSDashboardServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonEKSFargatePodExecutionRolePolicy

描述：提供在 AWS Fargate 上執行 Amazon EKS Pod 所需的其他 AWS 服務資源的存取權

AmazonEKSFargatePodExecutionRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSFargatePodExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 11 月 22 日 04：34 UTC
- 編輯時間：2019 年 11 月 22 日 04：34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEKSForFargateServiceRolePolicy

描述：此政策授予 Amazon EKS 執行 Fargate 任務的必要許可

`AmazonEKSForFargateServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 22 日 04：36 UTC
- 編輯時間：2019 年 11 月 22 日 04：36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSLoadBalancingPolicy

描述：連接到 EKS 叢集角色的政策，授予管理叢集負載平衡資源的許可。

AmazonEKSLoadBalancingPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSLoadBalancingPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 10 月 30 日 20：18 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSLoadBalancingPolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateRule",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group-rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateTargetGroup",
            "CreateListener",
            "CreateRule"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:SetIpAddressType",
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:SetSubnets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:ModifyListenerAttributes",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
```

```
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:DeleteProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:TagResource"
      ],
      "Resource" : "arn:aws:shield::*:protection/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPoolClient",
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "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:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSLocalOutpostClusterPolicy

描述：此政策提供許可給在您帳戶中執行的 EKS 本機叢集控制平面執行個體，以代表您管理資源。

AmazonEKSLocalOutpostClusterPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSLocalOutpostClusterPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 8 月 24 日，UTC 21：56
- 編輯時間：2024 年 10 月 24 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAvailabilityZones",
        "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/*:*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSLocalOutpostServiceRolePolicy

描述：允許 Amazon EKS Local 代表您呼叫 AWS 服務。

`AmazonEKSLocalOutpostServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 8 月 23 日，UTC 21：53
- 編輯時間：2025 年 6 月 26 日 18：22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
        "ssm:TerminateSession"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSMCPReadOnlyAccess

描述：提供 Amazon EKS MCP 服務的唯讀存取權。此政策授予在 EKS MCP 服務中僅使用唯讀工具的許可，旨在提供可觀測性、疑難排解、擷取 EKS 資源資訊，以及取得 EKS 最佳化建議。

AmazonEKSMCPReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSMCPReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 20 日 17：19 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSMCPReadOnlyAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListClusters",
        "eks:DescribeNodegroup",
        "eks:ListNodegroups",
        "eks:DescribeAddon",
        "eks:ListAddons",
        "eks:DescribeAccessEntry",
        "eks:ListAccessEntries",
        "eks:DescribeInsight",
        "eks:ListInsights",
        "eks:AccessKubernetesApi"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "eks-mcp:InvokeMcp",
        "eks-mcp:CallReadOnlyTool"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEKSNetworkingPolicy

描述：連接到 EKS 叢集角色的政策，授予管理叢集聯網資源的許可。

AmazonEKSNetworkingPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSNetworkingPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 10 月 28 日 22：34 UTC
- 編輯時間：2026 年 2 月 20 日 19：12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-cni-node-name" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-cni-node-name"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSServicePolicy

描述：此政策允許 Amazon Elastic Container Service for Kubernetes 建立和管理操作 EKS 叢集所需的資源。

AmazonEKSServicePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSServicePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 5 月 27 日，UTC 21：08
- 編輯時間：2024 年 10 月 14 日 21：12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSServicePolicy

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "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" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSServiceRolePolicy

描述：Amazon EKS 代表您呼叫 AWS 服務所需的服務連結角色。

AmazonEKSServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 2 月 21 日 20：10 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy

政策版本

政策版本： v23 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
```

```
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "eks:DescribeCluster",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTrustStores",
        "iam:ListAttachedRolePolicies",
        "pricing:GetProducts",
        "shield:GetSubscriptionState",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
```

```
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "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/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AWS/EKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry",
```

```
        "eks:DeleteAccessEntry"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "STANDARD"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : [
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputePolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputeClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSLoadBalancingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSLoadBalancingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSBlockStoragePolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSBlockStorageClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSHybridPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSEventPolicy"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "eks:DescribeAccessEntry",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "EC2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/EKS*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.ec2",
            "aws.health"
          ]
        },
        "StringEquals" : {
          "events:ManagedBy" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "arn:aws:events:*:*:rule/EKS*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "arn:aws:iam::*:instance-profile/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ManagedResourceOperator" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "ec2:DeleteSecurityGroup",
        "shield:DescribeProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSVPCResourceController

描述：VPC 資源控制器用來管理工作者節點 ENI 和 IPs的政策。

AmazonEKSVPCResourceController 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSVPCResourceController 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 8 月 12 日 00：55 UTC
- 編輯時間：2020 年 8 月 12 日 00：55 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSVPCResourceController

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEKSWorkerNodeMinimalPolicy

描述：此政策允許 Amazon EKS 工作者節點連線至 Amazon EKS 叢集。

AmazonEKSWorkerNodeMinimalPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSWorkerNodeMinimalPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 10 月 2 日 20：03 UTC
- 編輯時間：2024 年 10 月 2 日 20：03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEKSWorkerNodePolicy

描述：此政策允許 Amazon EKS 工作者節點連線至 Amazon EKS 叢集。

AmazonEKSWorkerNodePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonEKSWorkerNodePolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 5 月 27 日，UTC 21：09
- 編輯時間：2023 年 11 月 27 日 00：06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElastiCacheFullAccess

描述：透過 提供 Amazon ElastiCache 的完整存取權 AWS 管理主控台。

`AmazonElastiCacheFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElastiCacheFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC

- **編輯時間**：2023 年 11 月 28 日 03：49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : "elasticache:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/
AWSServiceRoleForElastiCache",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticache.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpoints",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
```

```
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToEc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowAccessToCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListLogDeliveryStreams",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowAccessToOutposts",
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElastiCacheReadOnlyAccess

描述：透過 提供 Amazon ElastiCache 的唯讀存取權 AWS 管理主控台。

`AmazonElastiCacheReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElastiCacheReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticContainerRegistryPublicFullAccess

描述：提供 Amazon ECR Public 資源的管理存取權

`AmazonElasticContainerRegistryPublicFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonElasticContainerRegistryPublicFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 1 日 17：25 UTC
- 編輯時間：2020 年 12 月 1 日 17：25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticContainerRegistryPublicPowerUser

描述：提供 Amazon ECR Public 儲存庫的完整存取權，但不允許刪除儲存庫或變更政策。

AmazonElasticContainerRegistryPublicPowerUser 是 AWS 受管政策。

使用此政策

您可以將 AmazonElasticContainerRegistryPublicPowerUser 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 1 日 16：16 UTC
- 編輯時間：2020 年 12 月 1 日 16：16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticContainerRegistryPublicReadOnly

描述：提供 Amazon ECR Public 儲存庫的唯讀存取權。

`AmazonElasticContainerRegistryPublicReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticContainerRegistryPublicReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 1 日 17：27 UTC

- **編輯時間**：2020 年 12 月 1 日 17：27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonElasticFileSystemClientFullAccess

描述：提供 Amazon EFS 檔案系統的根用戶端存取權

AmazonElasticFileSystemClientFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonElasticFileSystemClientFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 1 月 13 日 16：27 UTC
- 編輯時間：2020 年 1 月 13 日 16：27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticFileSystemClientReadOnlyAccess

描述：提供 Amazon EFS 檔案系統的唯讀用戶端存取權

`AmazonElasticFileSystemClientReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticFileSystemClientReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 1 月 13 日 16：24 UTC
- 編輯時間：2020 年 1 月 13 日 16：24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticFileSystemClientReadWriteAccess

描述：提供 Amazon EFS 檔案系統的讀取和寫入用戶端存取權

AmazonElasticFileSystemClientReadWriteAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonElasticFileSystemClientReadWriteAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 1 月 13 日 16：21 UTC
- 編輯時間：2020 年 1 月 13 日 16：21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonElasticFileSystemFullAccess

描述：透過 提供 Amazon EFS 的完整存取權 AWS 管理主控台。

`AmazonElasticFileSystemFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticFileSystemFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2015 年 5 月 27 日 16：22 UTC
- 編輯時間：2024 年 11 月 7 日 19：34 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemFullAccess",
      "Effect" : "Allow",
      "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",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEFS",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticfilesystem.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "IAMPassRoleAccessForEFS",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticfilesystem.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticFileSystemReadOnlyAccess

描述：透過 提供 Amazon EFS 的唯讀存取權 AWS 管理主控台。

`AmazonElasticFileSystemReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticFileSystemReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 5 月 27 日 16：25 UTC
- 編輯時間：2024 年 11 月 7 日 19：39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemReadOnlyAccess",
      "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",
        "elasticfilesystem:ReplicationRead",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticFileSystemServiceRolePolicy

描述：允許 Amazon Elastic File System 代表您管理 AWS 資源

`AmazonElasticFileSystemServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 5 日 16：52 UTC
- 編輯時間：2024 年 11 月 7 日 19：19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticFileSystemsUtils

描述：允許客戶使用 AWS Systems Manager 在 EC2 執行個體上自動管理 Amazon EFS 公用程式 (amazon-efs-utils) 套件，並使用 CloudWatchLog 取得 EFS 檔案系統掛載成功/失敗通知。

`AmazonElasticFileSystemsUtils` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticFileSystemsUtils` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 9 月 29 日 15：16 UTC
- 編輯時間：2020 年 9 月 29 日 15：16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticMapReduceEditorsRole

描述：Amazon Elastic MapReduce Editors 服務角色的預設政策。

`AmazonElasticMapReduceEditorsRole` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticMapReduceEditorsRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 11 月 16 日，UTC 21：55
- 編輯時間：2023 年 2 月 9 日 22：39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonElasticMapReduceforAutoScalingRole

描述：Amazon Elastic MapReduce for Auto Scaling。允許 Auto Scaling 從 EMR 叢集新增和移除執行個體的角色。

`AmazonElasticMapReduceforAutoScalingRole` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticMapReduceforAutoScalingRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 11 月 18 日 01：09 UTC
- 編輯時間：2016 年 11 月 18 日 01：09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticMapReduceforEC2Role

描述：Amazon Elastic MapReduce for EC2 服務角色的預設政策。

AmazonElasticMapReduceforEC2Role 是 AWS 受管政策。

使用此政策

您可以將 AmazonElasticMapReduceforEC2Role 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2017 年 8 月 11 日 23：57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticMapReduceFullAccess

描述：此政策位於棄用路徑上。如需指引，請參閱 文件：https：//https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html。提供 Amazon Elastic MapReduce 及其所需基礎服務的完整存取權，例如 EC2 和 S3

`AmazonElasticMapReduceFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticMapReduceFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2019 年 10 月 11 日 15：19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonElasticMapReducePlacementGroupPolicy

描述：允許 EMR 建立、描述和刪除 EC2 置放群組的政策。

AmazonElasticMapReducePlacementGroupPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonElasticMapReducePlacementGroupPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 9 月 29 日 00：37 UTC
- 編輯時間：2020 年 9 月 29 日 00：37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonElasticMapReduceReadOnlyAccess

描述：透過 提供 Amazon Elastic MapReduce 的唯讀存取權 AWS 管理主控台。

AmazonElasticMapReduceReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonElasticMapReduceReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2020 年 7 月 29 日，UTC 23：14
- ARN: arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonElasticMapReduceRole

描述：此政策位於棄用路徑上。如需指引，請參閱 文件：https：//https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html。Amazon Elastic MapReduce 服務角色的預設政策。

`AmazonElasticMapReduceRole` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticMapReduceRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2020 年 6 月 24 日，22：24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticsearchServiceRolePolicy

描述：允許 Amazon Elasticsearch Service 代表您存取其他 AWS 服務，例如 EC2 Networking APIs。

`AmazonElasticsearchServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 7 月 7 日 00：15 UTC
- 編輯時間：2023 年 10 月 23 日 06：58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonElasticTranscoder_FullAccess

描述：授予使用者對 Elastic Transcoder 的完整存取權，以及對 Elastic Transcoder 完整功能所需的相關服務的存取權。

AmazonElasticTranscoder_FullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonElasticTranscoder_FullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 4 月 27 日 18：59 UTC
- 編輯時間：2019 年 6 月 10 日 22：51 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticTranscoder_JobsSubmitter

描述：授予使用者變更預設集、提交任務和檢視 Elastic Transcoder 設定的許可。此政策也會授予一些使用 Elastic Transcode 主控台所需的其他服務的唯讀存取權，包括 S3、IAM 和 SNS。

`AmazonElasticTranscoder_JobsSubmitter` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticTranscoder_JobsSubmitter` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2018 年 6 月 7 日 21：12 UTC
- **編輯時間**：2019 年 6 月 10 日 22：49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticTranscoder_ReadOnlyAccess

描述：授予使用者對 Elastic Transcoder 的唯讀存取權，並列出對相關服務的存取權。

AmazonElasticTranscoder_ReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonElasticTranscoder_ReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 6 月 7 日，UTC 21：09
- 編輯時間：2019 年 6 月 10 日 22：48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonElasticTranscoderRole

描述：Amazon Elastic Transcoder 服務角色的預設政策。

`AmazonElasticTranscoderRole` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonElasticTranscoderRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2019 年 6 月 13 日 22：48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEMRCleanupPolicy

描述：允許 EMR 在 EMR Service 角色失去該功能時終止和刪除 AWS EC2 資源所需的動作。

`AmazonEMRCleanupPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 9 月 26 日 23：54 UTC
- 編輯時間：2020 年 9 月 29 日，UTC 21：11
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DeleteLaunchTemplate",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:CancelSpotInstanceRequests",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
```

```
        "ec2:DeleteVolume",
        "ec2:DescribePlacementGroups",
        "ec2:DeletePlacementGroup"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEMRContainersServiceRolePolicy

描述：允許存取執行 Amazon EMR 所需的其他 AWS 服務資源

AmazonEMRContainersServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 9 日 00：38 UTC
- 編輯時間：2025 年 2 月 6 日 21：07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation"
      ],
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEMRFullAccessPolicy_v2

描述：提供 Amazon EMR 的完整存取權

AmazonEMRFullAccessPolicy_v2 是 AWS 受管政策。

使用此政策

您可以將 AmazonEMRFullAccessPolicy_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 3 月 12 日 01：50 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:CreatePersistentAppUI",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteEditor",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEMRReadOnlyAccessPolicy_v2

描述：提供對 Amazon EMR 和相關聯 CloudWatch 指標的唯讀存取權。

AmazonEMRReadOnlyAccessPolicy_v2 是 AWS 受管政策。

使用此政策

您可以將 AmazonEMRReadOnlyAccessPolicy_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 3 月 12 日 01：39 UTC
- 編輯時間：2023 年 8 月 2 日 19：15 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEMRServerlessServiceRolePolicy

描述：允許存取執行 Amazon EMRServerless 所需的其他 AWS 服務資源

`AmazonEMRServerlessServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 5 月 20 日，UTC 23：15
- 編輯時間：2024 年 1 月 25 日 18：21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEMRServicePolicy_v2

描述：此政策用於 Amazon EMR Service 角色，不應用於帳戶中的任何其他 IAM 使用者或角色。此政策授予許可，以建立和管理與 EMR 相關的資源，以及 EMR 叢集操作所需的相關服務。

AmazonEMRServicePolicy_v2 是 AWS 受管政策。

使用此政策

您可以將 AmazonEMRServicePolicy_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 3 月 12 日 01：11 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
```

```
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
```

```
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
      "Sid" : "DeletePlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsForCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
```

```
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "CreateAndModifyEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
```

```
      }
    },
    {
      "Sid" : "TagEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonESCognitoAccess

描述：提供對 Amazon Cognito 組態服務的有限存取權。

AmazonESCognitoAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonESCognitoAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2018 年 2 月 28 日，UTC 22：29
- **編輯時間**：2021 年 12 月 20 日 14：04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonESFullAccess

描述：提供 Amazon ES 組態服務的完整存取權。

AmazonESFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonESFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 10 月 1 日 19：14 UTC
- 編輯時間：2015 年 10 月 1 日 19：14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonESFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonESReadOnlyAccess

描述：提供 Amazon ES 組態服務的唯讀存取權。

AmazonESReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonESReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2015 年 10 月 1 日 19：18 UTC
- **編輯時間**：2018 年 10 月 3 日 03：32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEventBridgeApiDestinationsServiceRolePolicy

描述：允許 EventBridge 代表您存取 Secret Manager 資源。

AmazonEventBridgeApiDestinationsServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 2 月 11 日 20：52 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:events!connection/*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/EventBridgeApiDestinations" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEventBridgeFullAccess

描述：提供 Amazon EventBridge 的完整存取權。

`AmazonEventBridgeFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEventBridgeFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 7 月 11 日 14：08 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEventBridgePipesFullAccess

描述：提供 Amazon EventBridge 管道的完整存取權。

`AmazonEventBridgePipesFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEventBridgePipesFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 12 月 1 日 17：03 UTC

- **編輯時間**：2022 年 12 月 1 日 17：03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEventBridgePipesOperatorAccess

描述：提供 Amazon EventBridge 管道的唯讀和運算子（停止和啟動執行管道的能力）存取權。

AmazonEventBridgePipesOperatorAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonEventBridgePipesOperatorAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 12 月 1 日 17：04 UTC
- 編輯時間：2022 年 12 月 1 日 17：04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess

政策版本

政策版本： v1（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEventBridgePipesReadOnlyAccess

描述：提供 Amazon EventBridge 管道的唯讀存取權。

`AmazonEventBridgePipesReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEventBridgePipesReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 12 月 1 日 17：04 UTC
- 編輯時間：2022 年 12 月 1 日 17：04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEventBridgeReadOnlyAccess

描述：提供 Amazon EventBridge 的唯讀存取權。

`AmazonEventBridgeReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEventBridgeReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 7 月 11 日 13：59 UTC

- **編輯時間**：2022 年 12 月 1 日 17：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonEventBridgeSchedulerFullAccess

描述：AmazonEventBridgeSchedulerFullAccess 受管政策授予許可，以使用排程和排程群組的所有 EventBridge 排程器動作。

`AmazonEventBridgeSchedulerFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEventBridgeSchedulerFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 11 月 10 日 18：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEventBridgeSchedulerReadOnlyAccess

描述：AmazonEventBridgeSchedulerReadOnlyAccess 受管政策授予唯讀許可，以檢視排程和排程群組的詳細資訊

`AmazonEventBridgeSchedulerReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEventBridgeSchedulerReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 10 日 18：50 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEventBridgeSchemasFullAccess

描述：提供 Amazon EventBridge 結構描述的完整存取權。

`AmazonEventBridgeSchemasFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEventBridgeSchemasFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 11 月 28 日 23：12 UTC
- 編輯時間：2019 年 11 月 28 日 23：12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEventBridgeSchemasReadOnlyAccess

描述：提供 Amazon EventBridge 結構描述的唯讀存取權。

`AmazonEventBridgeSchemasReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonEventBridgeSchemasReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 11 月 28 日 23：05 UTC
- 編輯時間：2020 年 5 月 1 日 00：50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEventBridgeSchemasServiceRolePolicy

描述：將許可授予 Amazon EventBridge 結構描述建立的受管規則。

AmazonEventBridgeSchemasServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 27 日 01：10 UTC
- 編輯時間：2019 年 11 月 27 日 01：10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonEVSServiceRolePolicy

描述：授予 EVS 代表您管理資源的許可

AmazonEVSServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 5 月 16 日 23：37 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonEVSServiceRolePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "ManageSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateEniWithTagStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "TagOnCreateNetworkInterface",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ManageInstanceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "DescribeInstanceAndVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "UpdateSecurityGroupStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "CloudWatchPutMetricDataStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/EVS"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonFISServiceRolePolicy

描述：讓 AWS FIS 管理實驗監控和資源選擇的政策。

AmazonFISServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 21 日 21：18 UTC
- 編輯時間：2022 年 10 月 25 日 09：05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonForecastFullAccess

描述：允許存取 Amazon Forecast 的所有動作

AmazonForecastFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonForecastFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 1 月 18 日 01：52 UTC
- 編輯時間：2019 年 1 月 18 日 01：52 UTC
- ARN: arn:aws:iam::aws:policy/AmazonForecastFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonFraudDetectorFullAccessPolicy

描述：允許存取 Amazon Fraud Detector 的所有動作

`AmazonFraudDetectorFullAccessPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonFraudDetectorFullAccessPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2019 年 12 月 3 日 22：46 UTC
- **編輯時間**：2019 年 12 月 3 日 22：46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonFreeRTOSFullAccess

描述：Amazon FreeRTOS 的完整存取政策

`AmazonFreeRTOSFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonFreeRTOSFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2017 年 11 月 29 日 15：32 UTC
- 編輯時間：2017 年 11 月 29 日 15：32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonFreeRTOSOTAUpdate

描述：允許使用者存取 Amazon FreeRTOS OTA 更新

`AmazonFreeRTOSOTAUpdate` 是 AWS 受管政策。

使用此政策

您可以將 AmazonFreeRTOSOTAUpdate 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 8 月 27 日，UTC 22：43
- 編輯時間：2020 年 12 月 18 日 17：47 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::afr-ota*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "signer:StartSigningJob",
        "signer:DescribeSigningJob",
        "signer:GetSigningProfile",
        "signer:PutSigningProfile"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteJob",
        "iot:DescribeJob"
      ],
      "Resource" : "arn:aws:iot:*:*:job/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream"
      ],
      "Resource" : "arn:aws:iot:*:*:stream/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateStream",
        "iot:CreateJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonFSxConsoleFullAccess

描述：提供 Amazon FSx 的完整存取權，以及透過 存取相關 AWS 服務 AWS 管理主控台。

AmazonFSxConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonFSxConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 11 月 28 日 16：36 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess

政策版本

政策版本： v20 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
```

```
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "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:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DetachAndDeleteS3AccessPoint",
        "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"
```

```
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonFSxConsoleReadOnlyAccess

描述：提供 Amazon FSx 的唯讀存取權，以及透過 存取相關 AWS 服務 AWS 管理主控台。

`AmazonFSxConsoleReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonFSxConsoleReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 28 日 16：35 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonFSxFullAccess

描述：提供 Amazon FSx 的完整存取權和相關 AWS 服務的存取權。

AmazonFSxFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonFSxFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 28 日 16：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonFSxFullAccess

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
```

```
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DetachAndDeleteS3AccessPoint",
        "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:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
```

```
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
      ]
    },
```

```
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonFSxReadOnlyAccess

描述：提供 Amazon FSx 的唯讀存取權。

AmazonFSxReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonFSxReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 28 日 16：33 UTC
- 編輯時間：2018 年 11 月 28 日 16：33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonFSxServiceRolePolicy

描述：允許 Amazon FSx 代表您管理 AWS 資源

AmazonFSxServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 28 日 10：38 UTC
- 編輯時間：2025 年 7 月 22 日 18：07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignIpv6Addresses",
        "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-*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonGlacierFullAccess

描述：透過 提供 Amazon Glacier 的完整存取權 AWS 管理主控台。

`AmazonGlacierFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonGlacierFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonGlacierReadOnlyAccess

描述：透過 提供 Amazon Glacier 的唯讀存取權 AWS 管理主控台。

`AmazonGlacierReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonGlacierReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2016 年 5 月 5 日 18：46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonGrafanaAthenaAccess

描述：此政策授予 Amazon Athena 的存取權，以及啟用從 Amazon Grafana 中的 Amazon Athena 外掛程式查詢和將結果寫入 s3 所需的相依性。

AmazonGrafanaAthenaAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonGrafanaAthenaAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 11 月 22 日 17：11 UTC
- 編輯時間：2021 年 11 月 22 日 17：11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonGrafanaCloudWatchAccess

描述：此政策會授予 Amazon CloudWatch 的存取權，以及使用 CloudWatch 做為 Amazon Managed Grafana 內資料來源所需的相依性。

`AmazonGrafanaCloudWatchAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonGrafanaCloudWatchAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 3 月 24 日 22：41 UTC
- 編輯時間：2023 年 3 月 24 日 22：41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonGrafanaRedshiftAccess

描述：此政策授予 Amazon Redshift 的範圍存取權，以及使用 Amazon Grafana 中的 Amazon Redshift 外掛程式所需的相依性。

AmazonGrafanaRedshiftAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonGrafanaRedshiftAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 11 月 26 日 23：15 UTC
- 編輯時間：2021 年 11 月 26 日 23：15 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonGrafanaServiceLinkedRolePolicy

描述：提供 Amazon Grafana 管理或使用 AWS 的資源存取權。

AmazonGrafanaServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 8 日 23：10 UTC
- 編輯時間：2022 年 11 月 8 日 23：10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonGuardDutyFullAccess

描述：提供使用 Amazon GuardDuty 的完整存取權。

AmazonGuardDutyFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonGuardDutyFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 28 日 22：31 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamGetRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
```

```
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonGuardDutyFullAccess_v2

描述：提供使用 Amazon GuardDuty 的完整存取權

AmazonGuardDutyFullAccess_v2 是 AWS 受管政策。

使用此政策

您可以將 AmazonGuardDutyFullAccess_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 6 月 4 日 20：22 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess_v2

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyFullAccess",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGuardDutyServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyOrganizationsAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
```

```
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyIamRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonGuardDutyMalwareProtectionServiceRolePolicy

描述：GuardDuty 惡意軟體保護使用名為 AWSServiceRoleForAmazonGuardDutyMalwareProtection 的服務連結角色 (SLR)。此服務連結角色可讓 GuardDuty 惡意軟體保護執行無代理程式掃描，以偵測惡意軟體。它允許 GuardDuty 在您的帳戶中建立快照，並與 GuardDuty 服務帳戶共用快照以掃描惡意軟體。它會評估這些共用快照，並在 GuardDuty 惡意軟體防護調查結果中包含擷取的 EC2 執行個體中繼資料。AWSServiceRoleForAmazonGuardDutyMalwareProtection 服務連結角色信任 malware-protection.guardduty.amazonaws.com 服務擔任該角色。

`AmazonGuardDutyMalwareProtectionServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 7 月 19 日 19：06 UTC
- 編輯時間：2024 年 1 月 25 日 22：24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonGuardDutyReadOnlyAccess

描述：提供 Amazon GuardDuty 資源的唯讀存取權

`AmazonGuardDutyReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonGuardDutyReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 28 日 22：29 UTC
- 編輯時間：2023 年 11 月 16 日 23：07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonGuardDutyServiceRolePolicy

描述：啟用存取 Amazon Guard Duty 使用或管理 AWS 的資源

AmazonGuardDutyServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 11 月 28 日 20：12 UTC
- 編輯時間：2024 年 8 月 12 日 20：01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        },
        "StringLike" : {
```

```
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.guardduty-data",
            "com.amazonaws.*.guardduty-data-fips"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutySecurityGroupManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/GuardDutyManaged" : "*"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateEksAddonPolicy",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEksAddonManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
    },
    {
      "Sid" : "GuardDutyEksClusterTagResourcePolicy",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
      "Effect" : "Allow",
      "Action" : "ecs:PutAccountSettingDefault",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:account-setting" : [
            "guardDutyActivate"
          ]
        }
      }
    },
    {
      "Sid" : "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation",
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmAddTagsToResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyManaged"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "SsmCreateUpdateAssociationInstanceDocumentPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
    },
    {
      "Sid" : "SsmSendCommandPermission",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin"
      ]
    },
    {
      "Sid" : "SsmGetCommandStatus",
      "Effect" : "Allow",
      "Action" : "ssm:GetCommandInvocation",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonHealthLakeFullAccess

描述：提供 Amazon HealthLake 服務的完整存取權。

`AmazonHealthLakeFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonHealthLakeFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 2 月 17 日 01：07 UTC
- 編輯時間：2021 年 2 月 17 日 01：07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonHealthLakeReadOnlyAccess

描述：提供 Amazon HealthLake 服務的唯讀存取權。

`AmazonHealthLakeReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonHealthLakeReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 2 月 17 日 02：43 UTC
- 編輯時間：2021 年 2 月 17 日 02：43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonHoneycodeFullAccess

描述：透過 AWS 管理主控台 和 SDK 提供 Honeycode 的完整存取權。

AmazonHoneycodeFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonHoneycodeFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 6 月 24 日，20：28 UTC
- 編輯時間：2020 年 6 月 24 日，20：28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonHoneycodeReadOnlyAccess

描述：透過 AWS 管理主控台 和 SDK 提供 Honeycode 的唯讀存取權。

AmazonHoneycodeReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonHoneycodeReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 6 月 24 日，20：28 UTC
- 編輯時間：2020 年 12 月 1 日 17：27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonHoneycodeServiceRolePolicy

描述：Amazon Honeycode 存取 資源所需的服務連結角色。

`AmazonHoneycodeServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 11 月 18 日 18：03 UTC
- 編輯時間：2020 年 11 月 18 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonHoneycodeTeamAssociationFullAccess

描述：透過 AWS 管理主控台 和 SDK 提供 Honeycode 團隊關聯的完整存取權。

AmazonHoneycodeTeamAssociationFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonHoneycodeTeamAssociationFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 6 月 24 日，20：28 UTC
- 編輯時間：2020 年 6 月 24 日，20：28 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonHoneycodeTeamAssociationReadOnlyAccess

描述：透過 AWS 管理主控台 和 SDK 提供 Honeycode Team Association 的唯讀存取權。

`AmazonHoneycodeTeamAssociationReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonHoneycodeTeamAssociationReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- 建立時間：2020 年 6 月 24 日，20：27 UTC
- 編輯時間：2020 年 6 月 24 日，20：27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonHoneycodeWorkbookFullAccess

描述：透過 AWS 管理主控台 和 SDK 提供 Honeycode 工作手冊的完整存取權。

`AmazonHoneycodeWorkbookFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonHoneycodeWorkbookFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 6 月 24 日，20：28 UTC
- 編輯時間：2020 年 12 月 1 日 17：30 UTC
- ARN: arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonHoneycodeWorkbookReadOnlyAccess

描述：透過 AWS 管理主控台 和 SDK 提供 Honeycode 工作手冊的唯讀存取權。

`AmazonHoneycodeWorkbookReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonHoneycodeWorkbookReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 6 月 24 日，20：28 UTC
- 編輯時間：2020 年 12 月 1 日 17：32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonInspector2AgentlessServiceRolePolicy

描述：授予 Amazon Inspector 執行無代理程式安全評估 AWS 服務 所需的存取權

`AmazonInspector2AgentlessServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 20 日 15：18 UTC
- 編輯時間：2023 年 11 月 20 日 15：18 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonInspector2FullAccess

描述：提供對 Amazon Inspector 的完整存取權，以及對組織等其他相關服務的存取權。

AmazonInspector2FullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonInspector2FullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 29 日 19：10 UTC
- 編輯時間：2024 年 4 月 25 日 13：21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2FullAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonInspector2FullAccess_v2

描述：提供 Amazon Inspector 的完整存取權，並存取其他相關服務，例如具有限制性組織存取權的組織。

AmazonInspector2FullAccess_v2 是 AWS 受管政策。

使用此政策

您可以將 AmazonInspector2FullAccess_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 7 月 3 日 16：07 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2FullAccess_v2

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowServicePrincipalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "inspector2.amazonaws.com",
            "agentless.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOrganizationalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:ou/o-*/ou-*"
```

```
    },
    {
      "Sid" : "AllowAccountsBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonInspector2ManagedCisPolicy

描述：這是受管政策，客戶應連接到其角色，以與 CIS 掃描的檢測器服務通訊

AmazonInspector2ManagedCisPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonInspector2ManagedCisPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 1 月 24 日 16：31 UTC
- 編輯時間：2024 年 1 月 24 日 16：31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonInspector2ManagedTelemetryPolicy

描述：授予與 Inspector2 遙測頻道通訊的許可

AmazonInspector2ManagedTelemetryPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonInspector2ManagedTelemetryPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2026 年 2 月 13 日 17：12 UTC
- 編輯時間：2026 年 2 月 13 日 17：12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedTelemetryPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForInspector2Telemetry",
      "Effect" : "Allow",
      "Action" : [
        "inspector2-telemetry:StartSession",
        "inspector2-telemetry:StopSession",
        "inspector2-telemetry:SendTelemetry",
        "inspector2-telemetry:NotifyHeartbeat"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonInspector2ReadOnlyAccess

描述：提供 Amazon inspector2 服務和相關支援服務的唯讀存取權

AmazonInspector2ReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonInspector2ReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 1 月 21 日 14：45 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonInspector2ServiceRolePolicy

描述：授予 Amazon Inspector 執行安全評估 AWS 服務 所需的存取權

`AmazonInspector2ServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 16 日 20：27 UTC
- 編輯時間：2026 年 2 月 13 日 17：12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

政策版本

政策版本： v26 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "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:DescribeFirewallMetadata",
        "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",
        "lambda:ListTags",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GatherInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce",
        "ssm:UpdateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "GatherInventoryDeleteAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "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" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToPutCloudwatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Inspector2"
        }
      }
    },
    {
      "Sid" : "AllowListAccessToECSAndEKS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters",
        "ecs:ListTasks",
        "eks:ListClusters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAccessToECSTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowInspectorEnablementForAwsOrgPolicy",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:AssociateMember"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceDelegatedAdminFromAwsOrg",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonInspectorFullAccess

描述：提供 Amazon Inspector 的完整存取權。

AmazonInspectorFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonInspectorFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 10 月 7 日 17：08 UTC
- 編輯時間：2017 年 12 月 21 日 14：53 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorFullAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonInspectorReadOnlyAccess

描述：提供 Amazon Inspector 的唯讀存取權。

AmazonInspectorReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonInspectorReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 10 月 7 日 17：08 UTC
- 編輯時間：2019 年 10 月 1 日 15：17 UTC
- ARN: arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonInspectorServiceRolePolicy

描述：授予 Amazon Inspector 執行安全評估 AWS 服務 所需的存取權

`AmazonInspectorServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 11 月 21 日 15：48 UTC
- 編輯時間：2020 年 9 月 11 日 17：12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonKendraFullAccess

描述：透過 提供 Amazon Kendra 的完整存取權 AWS 管理主控台。

AmazonKendraFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonKendraFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 16：15 UTC
- 編輯時間：2019 年 12 月 3 日 16：15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonKendraReadOnlyAccess

描述：透過 提供 Amazon Kendra 的唯讀存取權 AWS 管理主控台。

AmazonKendraReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonKendraReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 16：13 UTC
- 編輯時間：2021 年 5 月 27 日 17：01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kendra:Describe*",
        "kendra:List*",
        "kendra:Query",
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonKeyspacesFullAccess

描述：提供 Amazon Keyspaces 的完整存取權

AmazonKeyspacesFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonKeyspacesFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 4 月 23 日 17：06 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "KeyspacesCDCServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra-
streams.amazonaws.com/AWSServiceRoleForAmazonKeyspacesCDC",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra-streams.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonKeyspacesReadOnlyAccess

描述：提供 Amazon Keyspaces 的唯讀存取權

`AmazonKeyspacesReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonKeyspacesReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 4 月 23 日 17：07 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonKeyspacesReadOnlyAccess_v2

描述：提供 Amazon Keyspaces 和相關 AWS 服務的唯讀存取權。

AmazonKeyspacesReadOnlyAccess_v2 是 AWS 受管政策。

使用此政策

您可以將 AmazonKeyspacesReadOnlyAccess_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 9 月 12 日 17：01 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonKinesisAnalyticsFullAccess

描述：透過 提供 Amazon Kinesis Analytics 的完整存取權 AWS 管理主控台。

`AmazonKinesisAnalyticsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonKinesisAnalyticsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2016 年 9 月 21 日 19：01 UTC
- **編輯時間**：2016 年 9 月 21 日 19：01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonKinesisAnalyticsReadOnly

描述：透過 提供 Amazon Kinesis Analytics 的唯讀存取權 AWS 管理主控台。

`AmazonKinesisAnalyticsReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 AmazonKinesisAnalyticsReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2016 年 9 月 21 日 18：16 UTC
- 編輯時間：2016 年 9 月 21 日 18：16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonKinesisFirehoseFullAccess

描述：提供所有 Amazon Kinesis Firehose 交付串流的完整存取權。

AmazonKinesisFirehoseFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonKinesisFirehoseFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 10 月 7 日 18：45 UTC
- 編輯時間：2015 年 10 月 7 日 18：45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonKinesisFirehoseReadOnlyAccess

描述：提供所有 Amazon Kinesis Firehose 交付串流的唯讀存取權。

`AmazonKinesisFirehoseReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonKinesisFirehoseReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 10 月 7 日 18：43 UTC
- 編輯時間：2015 年 10 月 7 日 18：43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "firehose:Describe*",
        "firehose:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonKinesisFullAccess

描述：透過 提供所有串流的完整存取權 AWS 管理主控台。

AmazonKinesisFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonKinesisFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonKinesisReadOnlyAccess

描述：透過 提供所有串流的唯讀存取權 AWS 管理主控台。

AmazonKinesisReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonKinesisReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC

- **編輯時間**：2015 年 2 月 6 日 18：40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonKinesisVideoStreamsFullAccess

描述：透過 提供 Amazon Kinesis Video Streams 的完整存取權 AWS 管理主控台。

AmazonKinesisVideoStreamsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonKinesisVideoStreamsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 12 月 1 日 23：27 UTC
- 編輯時間：2017 年 12 月 1 日 23：27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonKinesisVideoStreamsReadOnlyAccess

描述：透過 提供 AWS Kinesis Video Streams 的唯讀存取權 AWS 管理主控台。

AmazonKinesisVideoStreamsReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonKinesisVideoStreamsReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 12 月 1 日 23：14 UTC
- 編輯時間：2017 年 12 月 1 日 23：14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*"
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonLaunchWizard_Fullaccess

描述： AWS 啟動精靈和其他必要服務的完整存取權。

AmazonLaunchWizard_Fullaccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonLaunchWizard_Fullaccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 8 月 6 日 17：47 UTC
- 編輯時間：2023 年 2 月 22 日 17：25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLaunchWizardFullAccessV2

描述： AWS 啟動精靈和其他必要服務的完整存取權。

AmazonLaunchWizardFullAccessV2 是 AWS 受管政策。

使用此政策

您可以將 AmazonLaunchWizardFullAccessV2 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 9 月 1 日 17：14 UTC
- 編輯時間：2023 年 9 月 1 日 17：14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLexChannelsAccess

描述：此政策允許客戶從頻道呼叫 Lex 執行期

AmazonLexChannelsAccess 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 1 月 13 日 20：12 UTC
- 編輯時間：2021 年 1 月 13 日 20：12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLexFullAccess

描述：透過 提供 Amazon Lex 的完整存取權 AWS 管理主控台。也提供建立 Lex 服務連結角色的存取權，並授予 Lex 呼叫一組有限 Lambda 函數的許可。

AmazonLexFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonLexFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 4 月 11 日 23：20 UTC
- 編輯時間：2024 年 4 月 16 日 20：06 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexFullAccess

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
```

```
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement4",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement5",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement6",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AmazonLexFullAccessStatement7",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement8",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "replication.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement9",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
```

```
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lex.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement12",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "channels.lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement13",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonLexReadOnly

描述：提供 Amazon Lex 的唯讀存取權。

`AmazonLexReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonLexReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 4 月 11 日 23：13 UTC
- 編輯時間：2024 年 5 月 13 日 16：58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexReadOnlyStatement1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotRecommendation",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:ListBots",
        "lex:ListBotLocales",
        "lex:ListBotAliases",
        "lex:ListBotAliasReplicas",
        "lex:ListBotChannels",
        "lex:ListBotRecommendations",
        "lex:ListBotReplicas",
        "lex:ListBotVersions",
        "lex:ListBotVersionReplicas",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
```

```
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListRecommendedIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "lex:SearchAssociatedTranscripts",
        "lex:ListCustomVocabularyItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonLexReplicationPolicy

描述：允許 Amazon Lex 代表您跨區域複寫 Lex 資源。

AmazonLexReplicationPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 1 月 31 日 23：29 UTC
- 編輯時間：2025 年 6 月 24 日 21：52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:ListTagsForResource",
        "lex:TagResource",
        "lex:UntagResource",
        "lex:CreateResourcePolicy",
        "lex:DeleteResourcePolicy",
        "lex:DescribeResourcePolicy",
        "lex:UpdateResourcePolicy"
      ],
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLexRunBotsOnly

描述：提供 Amazon Lex 對話式 APIs存取權。

AmazonLexRunBotsOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonLexRunBotsOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 4 月 11 日 23：06 UTC
- 編輯時間：2021 年 8 月 18 日 00：15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLexRunBotsOnly

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLexV2BotPolicy

描述：提供 Lex V2 機器人代表您呼叫其他 AWS 服務的存取權。

AmazonLexV2BotPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 1 月 13 日 20：10 UTC
- 編輯時間：2021 年 1 月 13 日 20：10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLookoutEquipmentFullAccess

描述：提供 Amazon Lookout for Equipment 操作的完整存取權

`AmazonLookoutEquipmentFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonLookoutEquipmentFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 4 月 8 日 15：52 UTC
- 編輯時間：2021 年 11 月 24 日 21：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonLookoutEquipmentReadOnlyAccess

描述：提供 Amazon Lookout for Equipments 的唯讀存取權

AmazonLookoutEquipmentReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonLookoutEquipmentReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 5 月 5 日 16：47 UTC
- 編輯時間：2022 年 11 月 10 日 22：04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonLookoutMetricsFullAccess

描述：允許存取 Amazon Lookout for Metrics 的所有動作

`AmazonLookoutMetricsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonLookoutMetricsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 5 月 7 日 00：43 UTC
- 編輯時間：2021 年 5 月 7 日 00：43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonLookoutMetricsReadOnlyAccess

描述：允許存取 Amazon Lookout for Metrics 的所有唯讀動作

`AmazonLookoutMetricsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonLookoutMetricsReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 5 月 7 日 00：43 UTC
- 編輯時間：2022 年 1 月 4 日 18：19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLookoutVisionConsoleFullAccess

描述：提供 Amazon Lookout for Vision 的完整存取權，以及對所需服務和主控台相依性的範圍存取權。

`AmazonLookoutVisionConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonLookoutVisionConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 5 月 11 日 19：37 UTC
- 編輯時間：2021 年 5 月 11 日 19：37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLookoutVisionConsoleReadOnlyAccess

描述：提供 Amazon Lookout for Vision 的唯讀存取權，以及對所需服務和主控台相依性的範圍存取權。

`AmazonLookoutVisionConsoleReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonLookoutVisionConsoleReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 5 月 11 日 19：32 UTC
- 編輯時間：2021 年 12 月 9 日，UTC 02：46
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLookoutVisionFullAccess

描述：提供 Amazon Lookout for Vision 的完整存取權，以及對必要相依性的範圍存取權。

AmazonLookoutVisionFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonLookoutVisionFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 5 月 11 日 19：24 UTC
- 編輯時間：2021 年 5 月 11 日 19：24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonLookoutVisionReadOnlyAccess

描述：提供 Amazon Lookout for Vision 的唯讀存取權，以及對必要相依性的範圍存取權。

`AmazonLookoutVisionReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonLookoutVisionReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 5 月 11 日 19：11 UTC
- 編輯時間：2021 年 12 月 9 日 03：01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMachineLearningBatchPredictionsAccess

描述：授予使用者請求 Amazon Machine Learning 批次預測的許可。

`AmazonMachineLearningBatchPredictionsAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMachineLearningBatchPredictionsAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 4 月 9 日 17：12 UTC
- 編輯時間：2015 年 4 月 9 日 17：12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMachineLearningCreateOnlyAccess

描述：提供非預測 Amazon Machine Learning 資源的建立存取權。

`AmazonMachineLearningCreateOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMachineLearningCreateOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 4 月 9 日 17：18 UTC
- 編輯時間：2016 年 6 月 29 日，UTC 20：55
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMachineLearningFullAccess

描述：提供 Amazon Machine Learning 資源的完整存取權。

`AmazonMachineLearningFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonMachineLearningFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 4 月 9 日 17：25 UTC
- 編輯時間：2015 年 4 月 9 日 17：25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

描述：授予使用者許可，以建立和刪除 Amazon Machine Learning 模型的即時端點。

AmazonMachineLearningManageRealTimeEndpointOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMachineLearningManageRealTimeEndpointOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 4 月 9 日 17：32 UTC
- 編輯時間：2015 年 4 月 9 日 17：32 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMachineLearningReadOnlyAccess

描述：提供 Amazon Machine Learning 資源的唯讀存取權。

`AmazonMachineLearningReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMachineLearningReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 4 月 9 日 17：40 UTC
- 編輯時間：2015 年 4 月 9 日 17：40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMachineLearningRealTimePredictionOnlyAccess

描述：授予使用者請求 Amazon Machine Learning 即時預測的許可。

AmazonMachineLearningRealTimePredictionOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMachineLearningRealTimePredictionOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 4 月 9 日 17：44 UTC

- **編輯時間**：2015 年 4 月 9 日 17：44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMachineLearningRoleforRedshiftDataSourceV3

描述：允許Machine Learning設定和使用您的 Redshift 叢集和 Redshift 資料來源的 S3 預備位置。

`AmazonMachineLearningRoleforRedshiftDataSourceV3` 是 AWS 受管政策。

使用此政策

您可以將 AmazonMachineLearningRoleforRedshiftDataSourceV3 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 6 月 24 日 18：00 UTC
- 編輯時間：2020 年 6 月 24 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMacieFullAccess

描述：提供 Amazon Macie 的完整存取權。

AmazonMacieFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMacieFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 8 月 14 日 14：54 UTC
- 編輯時間：2022 年 7 月 1 日 00：41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMacieFullAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMacieHandshakeRole

描述：准許建立 Amazon Macie 的服務連結角色。

AmazonMacieHandshakeRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonMacieHandshakeRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 6 月 28 日 15：46 UTC
- 編輯時間：2018 年 6 月 28 日 15：46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMacieReadOnlyAccess

描述：提供 Amazon Macie 的唯讀存取權。

`AmazonMacieReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMacieReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 6 月 15 日 21：50 UTC
- 編輯時間：2023 年 6 月 15 日 21：50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMacieServiceRole

描述：授予 Macie 對帳戶中資源相依性的唯讀存取權，以啟用資料分析。

AmazonMacieServiceRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonMacieServiceRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策

- 建立時間：2017 年 8 月 14 日 14：53 UTC
- 編輯時間：2017 年 8 月 14 日 14：53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMacieServiceRolePolicy

描述：Amazon Macie 的服務連結角色

AmazonMacieServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 6 月 19 日，UTC 22：17
- 編輯時間：2022 年 5 月 19 日 19：16 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonManagedBlockchainConsoleFullAccess

描述：透過 提供 Amazon Managed Blockchain 的完整存取權 AWS 管理主控台

AmazonManagedBlockchainConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonManagedBlockchainConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 4 月 29 日，UTC 21：23
- 編輯時間：2019 年 4 月 29 日，UTC 21：23
- ARN: arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonManagedBlockchainFullAccess

描述：提供 Amazon Managed Blockchain 的完整存取權。

`AmazonManagedBlockchainFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonManagedBlockchainFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 4 月 29 日，UTC 21：39
- 編輯時間：2019 年 4 月 29 日，UTC 21：39
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonManagedBlockchainReadOnlyAccess

描述：提供 Amazon Managed Blockchain 的唯讀存取權。

`AmazonManagedBlockchainReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonManagedBlockchainReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 4 月 30 日 18：17 UTC

- **編輯時間**：2019 年 4 月 30 日 18：17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonManagedBlockchainServiceRolePolicy

描述：允許存取 AWS 服務 Amazon Managed Blockchain 使用或管理的資源

AmazonManagedBlockchainServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 1 月 17 日 19：51 UTC
- 編輯時間：2020 年 1 月 17 日 19：51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonMCSFullAccess

描述：提供 Amazon Managed Apache Cassandra Service 的完整存取權

AmazonMCSFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMCSFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 13：45 UTC
- 編輯時間：2020 年 4 月 17 日，UTC 19：19
- ARN: arn:aws:iam::aws:policy/AmazonMCSFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMCSReadOnlyAccess

描述：提供 Amazon Managed Apache Cassandra Service 的唯讀存取權

AmazonMCSReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMCSReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 13：46 UTC
- 編輯時間：2020 年 4 月 17 日 19：21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMechanicalTurkFullAccess

描述：提供 Amazon Mechanical Turk 中所有 APIs 的完整存取權。

`AmazonMechanicalTurkFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonMechanicalTurkFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 12 月 11 日 19：08 UTC
- 編輯時間：2015 年 12 月 11 日 19：08 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMechanicalTurkReadOnly

描述：提供在 Amazon Mechanical Turk 中唯讀 APIs存取權。

AmazonMechanicalTurkReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonMechanicalTurkReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 12 月 11 日 19：08 UTC
- 編輯時間：2019 年 9 月 25 日，UTC 21：06
- ARN: arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMemoryDBFullAccess

描述：透過 提供 Amazon MemoryDB 的完整存取權 AWS 管理主控台。

`AmazonMemoryDBFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMemoryDBFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 10 月 8 日 19：24 UTC
- 編輯時間：2021 年 10 月 8 日 19：24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMemoryDBReadOnlyAccess

描述：透過 提供 Amazon MemoryDB 的唯讀存取權 AWS 管理主控台。

`AmazonMemoryDBReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonMemoryDBReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 10 月 8 日 19：27 UTC
- 編輯時間：2021 年 10 月 8 日 19：27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMobileAnalyticsFinancialReportAccess

描述：提供所有報告的唯讀存取權，包括所有應用程式資源的財務資料。

AmazonMobileAnalyticsFinancialReportAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMobileAnalyticsFinancialReportAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMobileAnalyticsFullAccess

描述：提供所有應用程式資源的完整存取權。

AmazonMobileAnalyticsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMobileAnalyticsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:*",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMobileAnalyticsNon-financialReportAccess

描述：為所有應用程式資源提供非財務報告的唯讀存取權。

AmazonMobileAnalyticsNon-financialReportAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMobileAnalyticsNon-financialReportAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMobileAnalyticsWriteOnlyAccess

描述：提供寫入存取，以放置所有應用程式資源的事件資料。（建議用於 SDK 整合）

`AmazonMobileAnalyticsWriteOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMobileAnalyticsWriteOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMonitronFullAccess

描述：提供管理 Amazon Monitron 的完整存取權

`AmazonMonitronFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMonitronFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 2 日，22：40 UTC
- 編輯時間：2022 年 6 月 8 日 16：27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMQApiFullAccess

描述：透過我們的 API/SDK 提供 AmazonMQ 的完整存取權。

`AmazonMQApiFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMQApiFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 12 月 18 日，UTC 20：31
- 編輯時間：2020 年 11 月 4 日 16：45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMQApiReadOnlyAccess

描述：透過我們的 API/SDK 提供 AmazonMQ 的唯讀存取權。

`AmazonMQApiReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMQApiReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 12 月 18 日，UTC 20：31
- 編輯時間：2018 年 12 月 18 日，20：31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMQFullAccess

描述：透過 提供 AmazonMQ 的完整存取權 AWS 管理主控台。

AmazonMQFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMQFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 11 月 28 日 15：28 UTC
- 編輯時間：2020 年 11 月 4 日 16：34 UTC

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

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMQReadOnlyAccess

描述：透過 提供 AmazonMQ 的唯讀存取權 AWS 管理主控台。

`AmazonMQReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMQReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 28 日 15：30 UTC
- 編輯時間：2017 年 11 月 28 日 19：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMQServiceRolePolicy

描述： AWS Amazon MQ 的服務連結角色政策

AmazonMQServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 11 月 4 日 16：07 UTC
- 編輯時間：2020 年 11 月 4 日 16：07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMSKConnectReadOnlyAccess

描述：提供 Amazon MSK Connect 的唯讀存取權

`AmazonMSKConnectReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonMSKConnectReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 9 月 20 日 10：18 UTC
- 編輯時間：2021 年 10 月 18 日 09：16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMSKFullAccess

描述：為其相依性提供 Amazon MSK 和其他必要許可的完整存取權。

AmazonMSKFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMSKFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 1 月 14 日 22：07 UTC
- 編輯時間：2023 年 10 月 18 日 11：33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonMSKFullAccess

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMSKReadOnlyAccess

描述：提供 Amazon MSK 的唯讀存取權

AmazonMSKReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonMSKReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 1 月 14 日 22：28 UTC
- 編輯時間：2019 年 1 月 14 日 22：28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonMWAAServerlessServiceRolePolicy

描述：提供 Amazon Airflow Serverless Service 的存取權，以管理工作流程的聯網，並代表您存取其他 AWS 服務

AmazonMWAAServerlessServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 11 月 15 日 20：34 UTC
- 編輯時間：2025 年 11 月 15 日 20：34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServerlessServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonMWAAServiceRolePolicy

描述：Amazon Managed Workflows for Apache Airflow 使用的服務連結角色。

AmazonMWAAServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 11 月 24 日 14：13 UTC
- 編輯時間：2022 年 11 月 17 日 00：56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonNimbleStudio-LaunchProfileWorker

描述：此政策會授予 Nimble Studio Launch Profile 工作者所需資源的存取權。將此政策連接至 Nimble Studio Builder 建立的 EC2 執行個體。

`AmazonNimbleStudio-LaunchProfileWorker` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonNimbleStudio-LaunchProfileWorker` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 4 月 28 日 04：47 UTC
- 編輯時間：2021 年 4 月 28 日 04：47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonNimbleStudio-StudioAdmin

描述：此政策會授予其他 服務中與 Studio 管理員和相關 Studio 資源相關聯的 Amazon Nimble Studio 資源的存取權。將此政策連接至與您的 Studio 相關聯的管理員角色。

AmazonNimbleStudio-StudioAdmin 是 AWS 受管政策。

使用此政策

您可以將 AmazonNimbleStudio-StudioAdmin 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 4 月 28 日 04：47 UTC
- 編輯時間：2023 年 9 月 22 日 17：40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonNimbleStudio-StudioUser

描述：此政策會授予其他 服務中與 Studio 使用者和相關 Studio 資源相關聯的 Amazon Nimble Studio 資源的存取權。將此政策連接至與您的 Studio 相關聯的使用者角色。

AmazonNimbleStudio-StudioUser 是 AWS 受管政策。

使用此政策

您可以將 AmazonNimbleStudio-StudioUser 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 4 月 28 日 04：48 UTC
- 編輯時間：2023 年 9 月 22 日 17：45 UTC
- ARN: arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonODBServiceRolePolicy

描述：允許 Oracle Database@ 代表您AWS 管理 AWS 資源。

AmazonODBServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 11 月 13 日 18：21 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC

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

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ODB"
          ]
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NM",
      "Effect" : "Allow",
```

```
      "Action" : [
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EB1",
      "Effect" : "Allow",
      "Action" : [
        "events:ActivateEventSource",
        "events:DescribeEventSource"
      ],
      "Resource" : "arn:aws:events:*:*:event-source/aws.partner/odb*"
    },
    {
      "Sid" : "EB2",
      "Effect" : "Allow",
      "Action" : [
        "events:CreateEventBus",
        "events:DescribeEventBus"
      ],
      "Resource" : "arn:aws:events:*:*:event-bus/aws.partner/odb*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonOmicsFullAccess

描述：提供 Amazon Omics 和其他必要項目的完整存取權 AWS 服務。此政策允許使用者檢視和接受 RAM 共用邀請，以存取使用者 外部的資源 AWS 帳戶。

AmazonOmicsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonOmicsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 2 月 24 日 00：59 UTC
- 編輯時間：2023 年 2 月 24 日 00：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOmicsFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonOmicsReadOnlyAccess

描述：提供 Amazon Omics 的唯讀存取權

`AmazonOmicsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonOmicsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 29 日 04：17 UTC

- **編輯時間**：2022 年 11 月 29 日 04：17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonOneEnterpriseFullAccess

描述：此政策會授予允許存取所有 Amazon One Enterprise 資源和操作的管理許可。

`AmazonOneEnterpriseFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonOneEnterpriseFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 11 月 28 日 04：58 UTC
- 編輯時間：2023 年 11 月 28 日 04：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonOneEnterpriseInstallerAccess

描述：此政策會授予有限的讀取和寫入許可，以允許裝置安裝和啟用。

AmazonOneEnterpriseInstallerAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonOneEnterpriseInstallerAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 11 月 28 日 05：00 UTC
- 編輯時間：2023 年 11 月 28 日 05：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
```

```
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonOneEnterpriseReadOnlyAccess

描述：此政策會授予所有 Amazon One Enterprise 資源和操作的唯讀許可。

`AmazonOneEnterpriseReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonOneEnterpriseReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 11 月 28 日 04：59 UTC
- 編輯時間：2023 年 11 月 28 日 04：59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonOpenSearchDashboardsServiceRolePolicy

描述：提供 Amazon OpenSearch Dashboards Service 的存取權，以代表您存取 CloudWatch AWS 等其他服務

`AmazonOpenSearchDashboardsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 12 月 22 日 19：38 UTC
- 編輯時間：2023 年 12 月 22 日 19：38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonOpenSearchDirectQueryGlueCreateAccess

描述：允許 OpenSearch DirectQuery Service 存取 AWS Glue APIs，以代表您建立資源。

AmazonOpenSearchDirectQueryGlueCreateAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonOpenSearchDirectQueryGlueCreateAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 5 月 6 日 12：24 UTC
- 編輯時間：2024 年 5 月 6 日 12：24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonOpenSearchIngestionFullAccess

描述：允許 Amazon OpenSearch Ingestion 代表您存取其他 AWS 服務。

`AmazonOpenSearchIngestionFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonOpenSearchIngestionFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 4 月 26 日 18：11 UTC
- 編輯時間：2023 年 4 月 26 日 18：11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonOpenSearchIngestionReadOnlyAccess

描述：提供 Amazon OpenSearch Ingestion Service 的唯讀存取權

`AmazonOpenSearchIngestionReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonOpenSearchIngestionReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 4 月 26 日 18：09 UTC
- 編輯時間：2023 年 4 月 26 日 18：09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonOpenSearchIngestionServiceRolePolicy

描述：允許 Amazon OpenSearch Ingestion Service 代表您存取其他 AWS 服務。

`AmazonOpenSearchIngestionServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 18 日 16：49 UTC
- 編輯時間：2025 年 8 月 28 日 18：19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:ModifyVpcEndpoint",
        "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"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonOpenSearchServerlessServiceRolePolicy

描述：允許 Amazon OpenSearch Serverless 代表您存取其他 AWS 服務，例如 CloudWatch APIs。

AmazonOpenSearchServerlessServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 24 日 19：50 UTC
- 編輯時間：2024 年 7 月 25 日 21：19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonOpenSearchServiceCognitoAccess

描述：提供 Amazon Cognito 組態服務的存取權。

`AmazonOpenSearchServiceCognitoAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonOpenSearchServiceCognitoAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 9 月 2 日 06：31 UTC
- 編輯時間：2021 年 12 月 20 日 14：04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonOpenSearchServiceFullAccess

描述：提供 Amazon OpenSearch Service 組態服務的完整存取權。

AmazonOpenSearchServiceFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonOpenSearchServiceFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 9 月 8 日 05：33 UTC
- 編輯時間：2021 年 9 月 8 日 05：33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonOpenSearchServiceReadOnlyAccess

描述：提供 Amazon OpenSearch Service 組態服務的唯讀存取權。

AmazonOpenSearchServiceReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonOpenSearchServiceReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 9 月 8 日 05：38 UTC
- 編輯時間：2021 年 9 月 8 日 05：38 UTC
- ARN: arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonOpenSearchServiceRolePolicy

描述：允許 Amazon OpenSearch Service 代表您存取其他 AWS 服務，例如 EC2 Networking APIs。

`AmazonOpenSearchServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 8 月 26 日 09：27 UTC

- **編輯時間**：2025 年 3 月 27 日，UTC 22：52
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
            "AWS/OpenSearch"
          ]
        }
      }
    },
    {
      "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"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sso:PutApplicationAccessScope",
      "Resource" : "arn:aws:sso::*:application/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    }
```

```
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonPersonalizeFullAccess

描述：透過 AWS 管理主控台 和 SDK 提供 Amazon Personalize 的完整存取權。也提供相關服務的選取存取權 （ 例如 S3、CloudWatch)。

AmazonPersonalizeFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonPersonalizeFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 12 月 4 日 22：24 UTC
- 編輯時間：2019 年 5 月 30 日 23：46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess

政策版本

政策版本： v2 （ 預設 ）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonPollyFullAccess

描述：授予 Amazon Polly 服務和資源的完整存取權。

AmazonPollyFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonPollyFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 11 月 30 日 18：59 UTC
- 編輯時間：2016 年 11 月 30 日 18：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "polly:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonPollyReadOnlyAccess

描述：授予 Amazon Polly 資源的唯讀存取權。

AmazonPollyReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonPollyReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 11 月 30 日 18：59 UTC
- 編輯時間：2018 年 7 月 17 日 16：41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonPrometheusConsoleFullAccess

描述：授予 AWS 主控台中 AWS 受管 Prometheus 資源的完整存取權

`AmazonPrometheusConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonPrometheusConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 15 日 18：11 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "aps:UpdateWorkspaceConfiguration",
        "aps:DescribeWorkspaceConfiguration",
        "aps:CreateQueryLoggingConfiguration",
        "aps:UpdateQueryLoggingConfiguration",
        "aps:DeleteQueryLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonPrometheusFullAccess

描述：授予 AWS 受管 Prometheus 資源的完整存取權

AmazonPrometheusFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonPrometheusFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 15 日 18：10 UTC
- 編輯時間：2023 年 11 月 26 日 20：16 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scraper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonPrometheusQueryAccess

描述：授予對 AWS Managed Prometheus 資源執行查詢的存取權

AmazonPrometheusQueryAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonPrometheusQueryAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 19 日 01：02 UTC
- 編輯時間：2020 年 12 月 19 日 01：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonPrometheusRemoteWriteAccess

描述：授予僅寫入 AWS 受管 Prometheus 工作區的存取權

AmazonPrometheusRemoteWriteAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonPrometheusRemoteWriteAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 19 日 01：04 UTC
- 編輯時間：2020 年 12 月 19 日 01：04 UTC
- ARN: arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonPrometheusScraperServiceRolePolicy

描述：提供存取由 Amazon Managed Service for Prometheus Collector 管理或使用 AWS 的資源

`AmazonPrometheusScraperServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 26 日 14：19 UTC
- 編輯時間：2024 年 4 月 26 日 20：25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AMPAgentlessScraper" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "ENIUpdating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "EKSAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DeleteEKSAccessEntry",
      "Effect" : "Allow",
      "Action" : "eks:DeleteAccessEntry",
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
        }
      }
    },
    {
      "Sid" : "APSWriting",
      "Effect" : "Allow",
      "Action" : "aps:RemoteWrite",
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonQDeveloperAccess

描述：提供開發人員存取權，以啟用與 Amazon Q 的互動

AmazonQDeveloperAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonQDeveloperAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 7 月 9 日 08：35 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQDeveloperAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:GetTroubleshootingResults",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetaData",
        "q:GenerateCodeFromCommands",
        "q:UsePlugin"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonQFullAccess

描述：提供完整存取權，以啟用與 Amazon Q 的互動

AmazonQFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonQFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 11 月 28 日 16：00 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonQFullAccess

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetadata",
        "q:CreateAssignment",
        "q:DeleteAssignment",
        "q:GenerateCodeFromCommands",
        "q:CreatePlugin",
        "q:UpdatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin",
        "q:UsePlugin",
        "q:ListPlugins",
        "q:ListPluginProviders",
        "q:ListTagsForResource",
        "q:UntagResource",
        "q:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonQLDBConsoleFullAccess

描述：透過 提供 Amazon QLDB 的完整存取權 AWS 管理主控台。

AmazonQLDBConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonQLDBConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 9 月 5 日 18：24 UTC
- 編輯時間：2022 年 11 月 4 日 17：01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonQLDBFullAccess

描述：透過服務 API 提供 Amazon QLDB 的完整存取權。

`AmazonQLDBFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonQLDBFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 9 月 5 日 18：23 UTC
- 編輯時間：2022 年 11 月 4 日 17：01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonQLDBReadOnly

描述：提供 Amazon QLDB 的唯讀存取權。

AmazonQLDBReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonQLDBReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 9 月 5 日 18：19 UTC
- 編輯時間：2021 年 7 月 2 日，UTC 02：17
- ARN: arn:aws:iam::aws:policy/AmazonQLDBReadOnly

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRDSBetaServiceRolePolicy

描述：允許 Amazon RDS 代表您管理 AWS 資源。

AmazonRDSBetaServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 5 月 2 日 19：41 UTC
- 編輯時間：2024 年 8 月 7 日 00：54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRDSCustomInstanceProfileRolePolicy

描述：允許 Amazon RDS Custom 透過 EC2 執行個體描述檔執行各種自動化動作和資料庫管理任務。

`AmazonRDSCustomInstanceProfileRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRDSCustomInstanceProfileRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 2 月 27 日 17：42 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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-*",
        "arn:aws:secretsmanager:*:*:secret: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-*",
            "arn:aws:secretsmanager:*:*:secret: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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRDSCustomPreviewServiceRolePolicy

描述：Amazon RDS 自訂預覽服務角色政策

AmazonRDSCustomPreviewServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 10 月 8 日，UTC 21：44
- 編輯時間：2026 年 2 月 12 日 17：58 UTC

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

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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-*",
        "arn:aws:ec2:*:*:key-pair/preview-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-*",
        "arn:aws:ec2:*:*:key-pair/preview-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: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" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/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-*",
        "arn:aws:secretsmanager:*:*:secret:preview-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",
        "secretsmanager:RestoreSecret"
```

```
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
```

```
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
    },
    {
      "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-oracle"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRDSCustomServiceRolePolicy

描述：允許 Amazon RDS Custom 代表您管理 AWS 資源。

AmazonRDSCustomServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 10 月 8 日，UTC 21：39
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

政策版本

政策版本： v19 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "rdscrc",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
```

```
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "eccModifyInstanceAttribute1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ],
          "ec2:Attribute" : "InstanceType"
        }
      }
    },
    {
```

```
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/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-*",
```

```
        "arn:aws:ec2:*:*:key-pair/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",
            "CopyImage"
```

```
          ]
        }
      }
    },
    {
      "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: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" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccAmi1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ]
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
```

```
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSRDSCustom*",
        "arn:aws:iam::*:role/service-role/AWSRDSCustom*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret: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",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "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",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "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",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonRDSDataFullAccess

描述：允許完整存取使用 RDS 資料 APIs、RDS 資料庫登入資料的秘密存放APIs，以及資料庫主控台查詢管理 APIs，以在 中的 Aurora Serverless 叢集上執行 SQL 陳述式 AWS 帳戶。

`AmazonRDSDataFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRDSDataFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 20 日，UTC 21：29
- 編輯時間：2019 年 11 月 20 日 21：58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRDSDirectoryServiceAccess

描述：允許 RDS 代表客戶存取加入網域的 SQL Server 資料庫執行個體的 Directory Service Managed AD。

`AmazonRDSDirectoryServiceAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRDSDirectoryServiceAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 2 月 26 日 02：02 UTC
- 編輯時間：2019 年 5 月 15 日 16：51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRDSEnhancedMonitoringRole

描述：提供存取 Cloudwatch 以進行 RDS 增強型監控

AmazonRDSEnhancedMonitoringRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonRDSEnhancedMonitoringRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 11 月 11 日 19：58 UTC
- 編輯時間：2015 年 11 月 11 日 19：58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRDSFullAccess

描述：透過 提供 Amazon RDS 的完整存取權 AWS 管理主控台。

`AmazonRDSFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRDSFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2023 年 8 月 17 日 23：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRDSPerformanceInsightsFullAccess

描述：透過 提供 RDS Performance Insights 的完整存取權 AWS 管理主控台

`AmazonRDSPerformanceInsightsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRDSPerformanceInsightsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 8 月 15 日 23：41 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "rds:ListTagsForResource",
        "rds:DescribeDBShardGroups"
      ],
```

```
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:shard-group:*"
      ]
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRDSPerformanceInsightsReadOnly

描述：RDS Performance Insights 的唯讀政策

AmazonRDSPerformanceInsightsReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonRDSPerformanceInsightsReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 4 月 5 日 00：02 UTC

- **編輯時間**：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBShardGroups",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBShardGroups",
      "Resource" : "arn:aws:rds:*:*:shard-group:*"
    },
    {
      "Sid" : "AmazonRDSListTagsForResource",
      "Effect" : "Allow",
      "Action" : "rds:ListTagsForResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:shard-group:*",
        "arn:aws:rds:*:*:cluster:*"
      ]
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRDSPreviewServiceRolePolicy

描述：Amazon RDS 預覽服務角色政策

AmazonRDSPreviewServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 5 月 31 日 18：02 UTC
- 編輯時間：2024 年 8 月 7 日 01：02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
        "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"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRDSReadOnlyAccess

描述：透過 提供 Amazon RDS 的唯讀存取權 AWS 管理主控台。

`AmazonRDSReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRDSReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2023 年 4 月 14 日 12：32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "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"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRDSServiceRolePolicy

描述：允許 Amazon RDS 代表您管理 AWS 資源。

`AmazonRDSServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 1 月 8 日 18：17 UTC
- 編輯時間：2024 年 7 月 1 日 22：42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRedshiftAllCommandsFullAccess

描述：此政策包含執行 SQL 命令的許可，以在 Amazon Redshift 上複製、載入、卸載、查詢和分析資料。此政策也授予許可，以執行相關服務的選取陳述式，例如 Amazon S3、Amazon CloudWatch logs、Amazon SageMaker 或 AWS Glue。

`AmazonRedshiftAllCommandsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRedshiftAllCommandsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 4 日 00：48 UTC
- 編輯時間：2021 年 11 月 25 日 02：27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRedshiftDataFullAccess

描述：此政策提供 Amazon Redshift 資料 APIs 的完整存取權。此政策也會授予其他必要服務的範圍存取權。

AmazonRedshiftDataFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRedshiftDataFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 9 月 9 日 19：23 UTC
- 編輯時間：2023 年 4 月 7 日 18：18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRedshiftFederatedAuthorization

描述：這是使用 Amazon Redshift 聯合授權執行查詢的ease-of-use政策

AmazonRedshiftFederatedAuthorization 是 AWS 受管政策。

使用此政策

您可以將 AmazonRedshiftFederatedAuthorization 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 22 日 00：04 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftFederatedAuthorization

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftFederatedAuthorization",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetUserDefinedFunctions",
        "glue:CreateDatabase",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeleteTable",
        "glue:UpdateCatalog",
        "glue:UpdateDatabase",
```

```
        "glue:UpdateTable",
        "glue:RenameTable",
        "glue:FederateAuthorization"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:FederatedAuthorizationSource" : "Redshift"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftIdentityCenterSetContext",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRedshiftFullAccess

描述：透過 提供 Amazon Redshift 的完整存取權 AWS 管理主控台。

AmazonRedshiftFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRedshiftFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2022 年 7 月 7 日 23：31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRedshiftQueryEditor

描述：提供 Amazon Redshift 查詢編輯器的完整存取權，以及透過 儲存的查詢 AWS 管理主控台。

AmazonRedshiftQueryEditor 是 AWS 受管政策。

使用此政策

您可以將 AmazonRedshiftQueryEditor 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 10 月 4 日，UTC 22：50
- 編輯時間：2021 年 2 月 16 日 19：33 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRedshiftQueryEditorV2FullAccess

描述：授予 Amazon Redshift 查詢編輯器 V2 操作和資源的完整存取權。此政策也會授予其他必要服務的存取權。這包括在 AWS KMS 中列出 Amazon Redshift 叢集、讀取金鑰和別名，以及在 AWS Secrets Manager 中管理查詢編輯器 V2 秘密的許可。

`AmazonRedshiftQueryEditorV2FullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRedshiftQueryEditorV2FullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 9 月 24 日 14：06 UTC
- 編輯時間：2024 年 2 月 21 日 17：20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRedshiftQueryEditorV2NoSharing

描述：授予在不共用資源的情況下使用 Amazon Redshift 查詢編輯器 V2 的能力。授予的委託人只能讀取、更新和刪除自己的資源，但無法共用它們。此政策也會授予其他必要服務的存取權。這包括在 Secrets Manager 中列出 Amazon Redshift 叢集和管理主體之查詢編輯器 V2 AWS 秘密的許可。

`AmazonRedshiftQueryEditorV2NoSharing` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRedshiftQueryEditorV2NoSharing` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 9 月 24 日 14：18 UTC
- 編輯時間：2024 年 2 月 21 日 17：25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
```

```
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
```

```
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRedshiftQueryEditorV2ReadSharing

描述：授予使用 Amazon Redshift 查詢編輯器 V2 和有限資源共用的能力。授予的委託人可以讀取、寫入和共用自己的資源。授予的委託人可以讀取與其團隊共用的資源，但無法更新這些資源。此政策也會

授予其他必要服務的存取權。這包括在 Secrets Manager 中列出 Amazon Redshift 叢集和管理主體之查詢編輯器 V2 AWS 秘密的許可。

AmazonRedshiftQueryEditorV2ReadSharing 是 AWS 受管政策。

使用此政策

您可以將 AmazonRedshiftQueryEditorV2ReadSharing 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 9 月 24 日 14：22 UTC
- 編輯時間：2024 年 2 月 21 日 17：27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
```

```
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
```

```
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
```

```
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRedshiftQueryEditorV2ReadWriteSharing

描述：授予使用 Amazon Redshift 查詢編輯器 V2 與資源共用的能力。授予的委託人可以讀取、寫入和共用自己的資源。獲得授予的主體可以讀取和更新與其團隊共用的資源。此政策也會授予其他必要服務的存取權。這包括在 Secrets Manager 中列出 Amazon Redshift 叢集和管理主體之查詢編輯器 V2 AWS 秘密的許可。

`AmazonRedshiftQueryEditorV2ReadWriteSharing` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRedshiftQueryEditorV2ReadWriteSharing` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2021 年 9 月 24 日 14：25 UTC
- **編輯時間**：2024 年 2 月 21 日 17：30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
```

```
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
```

```
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
```

```
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRedshiftReadOnlyAccess

描述：透過 提供 Amazon Redshift 的唯讀存取權 AWS 管理主控台。

`AmazonRedshiftReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRedshiftReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2024 年 2 月 8 日 00：24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRedshiftServiceLinkedRolePolicy

描述：允許 Amazon Redshift 代表您呼叫 AWS 服務

AmazonRedshiftServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 9 月 18 日 19：19 UTC
- 編輯時間：2025 年 2 月 19 日 17：22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
      ]
    },
    {
      "Sid" : "DiscoverRedshiftCatalogs",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:GetCatalog",
        "glue:GetCatalogs"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Bool" : {
          "glue:EnabledForRedshiftAutoDiscovery" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeFormationGetMetadataAccessForFederatedCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Bool" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "glue.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRekognitionCustomLabelsFullAccess

描述：此政策指定 Amazon Rekognition 自訂標籤功能所需的 rekognition 和 s3 許可。

AmazonRekognitionCustomLabelsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRekognitionCustomLabelsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 1 月 8 日 19：18 UTC
- 編輯時間：2022 年 8 月 16 日 20：20 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRekognitionFullAccess

描述：存取所有 Amazon Rekognition APIs

AmazonRekognitionFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRekognitionFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 11 月 30 日 14：40 UTC
- 編輯時間：2016 年 11 月 30 日 14：40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRekognitionFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRekognitionReadOnlyAccess

描述：存取所有 Read rekognition APIs

`AmazonRekognitionReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRekognitionReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2016 年 11 月 30 日 14：58 UTC
- 編輯時間：2023 年 11 月 8 日 18：30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRekognitionServiceRole

描述：允許 Rekognition 代表您呼叫 AWS 服務。

AmazonRekognitionServiceRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonRekognitionServiceRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 11 月 29 日 16：52 UTC
- 編輯時間：2017 年 11 月 29 日 16：52 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRoute53AutoNamingFullAccess

描述：提供所有 Route 53 Auto 命名動作的完整存取權。

AmazonRoute53AutoNamingFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53AutoNamingFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 1 月 18 日 18：40 UTC
- 編輯時間：2018 年 1 月 18 日 18：40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53AutoNamingReadOnlyAccess

描述：提供所有 Route 53 Auto 命名動作的唯讀存取權。

`AmazonRoute53AutoNamingReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRoute53AutoNamingReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 1 月 18 日 03：02 UTC
- 編輯時間：2018 年 1 月 18 日 03：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53AutoNamingRegistrantAccess

描述：提供 Route 53 Auto Naming 動作的註冊者層級存取權。

`AmazonRoute53AutoNamingRegistrantAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53AutoNamingRegistrantAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 3 月 12 日，UTC 22：33
- 編輯時間：2018 年 3 月 12 日，UTC 22：33
- ARN: arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53DomainsFullAccess

描述：提供所有 Route53 網域動作和建立託管區域的完整存取權，以允許建立託管區域作為網域註冊的一部分。

AmazonRoute53DomainsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53DomainsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53DomainsReadOnlyAccess

描述：提供 Route53 網域清單和動作的存取權。

`AmazonRoute53DomainsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRoute53DomainsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC

- **編輯時間**：2015 年 2 月 6 日 18：40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRoute53FullAccess

描述：透過 提供所有 Amazon Route 53 的完整存取權 AWS 管理主控台。

AmazonRoute53FullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53FullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53FullAccess

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistributionTenantByDomain",
        "cloudfront:GetConnectionGroup",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "es:ListDomainNames",
        "es:DescribeDomains",
        "lightsail:GetContainerServices",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53GlobalResolverFullAccess

描述：提供擷取、列出、建立、更新和刪除所有 Amazon Route 53 Global Resolver 資源的完整存取權。

`AmazonRoute53GlobalResolverFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRoute53GlobalResolverFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2026 年 3 月 9 日 20：27 UTC
- 編輯時間：2026 年 3 月 9 日 20：27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53GlobalResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53globalresolver:AllowVendedLogDeliveryForResource",
        "route53globalresolver:AssociateHostedZone",
        "route53globalresolver:BatchCreateFirewallRule",
        "route53globalresolver:BatchDeleteFirewallRule",
        "route53globalresolver:BatchUpdateFirewallRule",
        "route53globalresolver:CreateAccessSource",
        "route53globalresolver:CreateAccessToken",
        "route53globalresolver:CreateDNSView",
        "route53globalresolver:CreateFirewallDomainList",
        "route53globalresolver:CreateFirewallRule",
        "route53globalresolver:CreateGlobalResolver",
        "route53globalresolver:DeleteAccessSource",
        "route53globalresolver:DeleteAccessToken",
        "route53globalresolver:DeleteDNSView",
        "route53globalresolver:DeleteFirewallDomainList",
```

```
        "route53globalresolver:DeleteFirewallRule",
        "route53globalresolver:DeleteGlobalResolver",
        "route53globalresolver:DisableDNSView",
        "route53globalresolver:DisassociateHostedZone",
        "route53globalresolver:EnableDNSView",
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetAccessToken",
        "route53globalresolver:GetDNSView",
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ImportFirewallDomains",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListManagedFirewallDomainLists",
        "route53globalresolver:ListTagsForResource",
        "route53globalresolver:TagResource",
        "route53globalresolver:UntagResource",
        "route53globalresolver:UpdateAccessSource",
        "route53globalresolver:UpdateAccessToken",
        "route53globalresolver:UpdateDNSView",
        "route53globalresolver:UpdateFirewallDomains",
        "route53globalresolver:UpdateFirewallRule",
        "route53globalresolver:UpdateGlobalResolver",
        "route53globalresolver:UpdateHostedZoneAssociation"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRoute53GlobalResolverReadOnlyAccess

描述：提供唯讀存取權，以擷取和列出所有 Amazon Route 53 Global Resolver 資源。

AmazonRoute53GlobalResolverReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53GlobalResolverReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2026 年 3 月 9 日 20：27 UTC
- 編輯時間：2026 年 3 月 9 日 20：27 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53GlobalResolverReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53GlobalResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53globalresolver:GetAccessSource",
        "route53globalresolver:GetAccessToken",
        "route53globalresolver:GetDNSView",
```

```
        "route53globalresolver:GetFirewallDomainList",
        "route53globalresolver:GetFirewallRule",
        "route53globalresolver:GetGlobalResolver",
        "route53globalresolver:GetHostedZoneAssociation",
        "route53globalresolver:GetManagedFirewallDomainList",
        "route53globalresolver:ListAccessSources",
        "route53globalresolver:ListAccessTokens",
        "route53globalresolver:ListDNSViews",
        "route53globalresolver:ListFirewallDomainLists",
        "route53globalresolver:ListFirewallDomains",
        "route53globalresolver:ListFirewallRules",
        "route53globalresolver:ListGlobalResolvers",
        "route53globalresolver:ListHostedZoneAssociations",
        "route53globalresolver:ListManagedFirewallDomainLists"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53ProfilesFullAccess

描述：此政策授予 Amazon Route 53 Profile 資源的完整存取權。

`AmazonRoute53ProfilesFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRoute53ProfilesFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2024 年 4 月 30 日 18：30 UTC
- 編輯時間：2024 年 8 月 27 日 19：18 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:CreateProfile",
        "route53profiles:DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53profiles:PutProfilePolicy",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
```

```
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRoute53ProfilesReadOnlyAccess

描述：此政策授予 Amazon Route 53 Profile 資源的唯讀存取權。

`AmazonRoute53ProfilesReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRoute53ProfilesReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 4 月 30 日 18：29 UTC
- 編輯時間：2024 年 8 月 27 日 18：59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53ReadOnlyAccess

描述：透過 提供所有 Amazon Route 53 的唯讀存取權 AWS 管理主控台。

AmazonRoute53ReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53ReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2016 年 11 月 15 日 21：15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53RecoveryClusterFullAccess

描述：提供 Amazon Route 53 復原叢集的完整存取權

`AmazonRoute53RecoveryClusterFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRoute53RecoveryClusterFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 8 月 18 日 18：37 UTC
- 編輯時間：2021 年 8 月 18 日 18：37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53RecoveryClusterReadOnlyAccess

描述：提供 Amazon Route 53 復原叢集的唯讀存取權

AmazonRoute53RecoveryClusterReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53RecoveryClusterReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 8 月 18 日 17：36 UTC
- 編輯時間：2022 年 4 月 1 日 17：37 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53RecoveryControlConfigFullAccess

描述：提供 Amazon Route 53 復原控制組態的完整存取權

`AmazonRoute53RecoveryControlConfigFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53RecoveryControlConfigFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 8 月 18 日 17：48 UTC
- 編輯時間：2021 年 8 月 18 日 17：48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53RecoveryControlConfigReadOnlyAccess

描述：提供 Amazon Route 53 復原控制組態的唯讀存取權

AmazonRoute53RecoveryControlConfigReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53RecoveryControlConfigReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 8 月 18 日 18：01 UTC
- 編輯時間：2023 年 10 月 18 日 17：15 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRoute53RecoveryReadinessFullAccess

描述：提供 Amazon Route 53 復原準備的完整存取權

AmazonRoute53RecoveryReadinessFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53RecoveryReadinessFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 8 月 18 日 16：45 UTC

- **編輯時間**：2021 年 8 月 18 日 16：45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53RecoveryReadinessReadOnlyAccess

描述：提供 Amazon Route 53 復原準備的唯讀存取權

`AmazonRoute53RecoveryReadinessReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53RecoveryReadinessReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 8 月 18 日 18：11 UTC
- 編輯時間：2021 年 11 月 9 日 20：14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
```

```
        "route53-recovery-readiness:ListTagsForResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonRoute53ResolverFullAccess

描述：Route 53 Resolver 的完整存取政策

`AmazonRoute53ResolverFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonRoute53ResolverFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 5 月 30 日 18：10 UTC
- 編輯時間：2024 年 8 月 5 日 20：06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonRoute53ResolverReadOnlyAccess

描述：Route 53 Resolver 的唯讀政策

AmazonRoute53ResolverReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonRoute53ResolverReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 5 月 30 日 18：11 UTC
- 編輯時間：2024 年 8 月 5 日 18：54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonS3FullAccess

描述：透過 提供所有儲存貯體的完整存取權 AWS 管理主控台。

AmazonS3FullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonS3FullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2021 年 9 月 27 日，UTC 20：16
- ARN: arn:aws:iam::aws:policy/AmazonS3FullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonS3ObjectLambdaExecutionRolePolicy

描述：提供 AWS Lambda 函數與 Amazon S3 Object Lambda 互動的許可。同時授予 Lambda 寫入 CloudWatch Logs 的許可。

AmazonS3ObjectLambdaExecutionRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonS3ObjectLambdaExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 8 月 18 日 10：07 UTC
- 編輯時間：2021 年 8 月 18 日 10：07 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonS3OutpostsFullAccess

描述：透過 提供 Amazon S3 on Outposts 的完整存取權 AWS 管理主控台。

AmazonS3OutpostsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonS3OutpostsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 10 月 2 日 17：26 UTC
- 編輯時間：2020 年 10 月 2 日 17：26 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonS3OutpostsReadOnlyAccess

描述：透過 提供 Amazon S3 on Outposts 的唯讀存取權 AWS 管理主控台。

`AmazonS3OutpostsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonS3OutpostsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2020 年 10 月 2 日 18：55 UTC
- **編輯時間**：2020 年 10 月 2 日 18：55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonS3ReadOnlyAccess

描述：透過 提供所有儲存貯體的唯讀存取權 AWS 管理主控台。

AmazonS3ReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonS3ReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2023 年 8 月 10 日 21：31 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

政策版本

政策版本： v3 （ 預設 ）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonS3TablesFullAccess

描述：提供所有 S3 資料表儲存貯體的完整存取權。

AmazonS3TablesFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonS3TablesFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 12 月 3 日 15：21 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3TablesFullAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToS3TablesReplication",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "replication.s3tables.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonS3TablesLakeFormationServiceRole

描述：此受管政策授予 AWS Lake Formation 許可，以對帳戶中的所有資料表儲存貯體、命名空間和資料表採取行動。

AmazonS3TablesLakeFormationServiceRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonS3TablesLakeFormationServiceRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 6 月 19 日 19：07 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonS3TablesLakeFormationServiceRole

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForS3ListTableBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:ListTableBuckets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:GetTableBucket",
        "s3tables:CreateNamespace",
        "s3tables:GetNamespace",
        "s3tables:ListNamespaces",
        "s3tables:DeleteNamespace",
        "s3tables:DeleteTableBucket",
        "s3tables:CreateTable",
        "s3tables:DeleteTable",
        "s3tables:GetTable",
        "s3tables:ListTables",
        "s3tables:RenameTable",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTableData",
        "s3tables:PutTableData",
```

```
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3tables:*:*:bucket/*/table/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDescribeKeyAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3tables.*.amazonaws.com"
          ]
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonS3TablesReadOnlyAccess

描述：提供所有 S3 資料表儲存貯體的唯讀存取權。

AmazonS3TablesReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonS3TablesReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 12 月 3 日 15：21 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonS3TablesReadOnlyAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:Get*",
        "s3tables:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

描述： AWS 服務 Catalog 服務用來從 Amazon SageMaker 產品組合佈建產品的服務角色政策。授予一組相關服務的許可，包括 CodePipeline、CodeBuild、CodeCommit、Glue、CloudFormation 等。

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 11 月 27 日 18：48 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPostPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPatchPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PATCH"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnMutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "ArnLikeIfExists" : {
          "cloudformation:RoleArn" : [
            "arn:aws:sts::*:assumed-role/AmazonSageMakerServiceCatalog*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
```

```
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTemplatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateCommit",
```

```
        "codecommit:CreateRepository",
        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitListPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodePipelinePermission",
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
      ],
      "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMUserPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateUserPool",
        "cognito-idp:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
```

```
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DescribeRule",
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogFirehosePermission",
      "Effect" : "Allow",
      "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGluePermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueClassiferPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateClassifier",
```

```
        "glue:DeleteClassifier",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeleteTrigger",
        "glue:DeleteWorkflow",
        "glue:StopCrawler"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueWorkflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateWorkflow"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueJobPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueCrawlerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:GetCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueTriggerPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaTagPermission",
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
```

```
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
        "arn:aws:logs:*:*:log-group::log-stream:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadPermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadSagemakerResourcePermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3MutatePermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
      ],
      "Resource" : "arn:aws:s3:::sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
        "sagemaker:CreateCodeRepository",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:DeleteCodeRepository"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*"
      ]
    },
    {
```

```
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateImage",
        "sagemaker:DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogStepFunctionPermission",
      "Effect" : "Allow",
      "Action" : [
        "states:CreateStateMachine",
        "states:DeleteStateMachine",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
```

```
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeStarPermission",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerCanvasAIServicesAccess

描述：提供 Amazon SageMaker Canvas 使用 AI 服務的許可，以支援隨時可用的 AI 解決方案。隨著 Amazon SageMaker Canvas 新增支援，此政策將為服務新增更多變動許可。

AmazonSageMakerCanvasAIServicesAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerCanvasAIServicesAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 3 月 23 日，UTC 22：36
- 編輯時間：2023 年 11 月 29 日 14：47 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Textract",
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument",
        "textract:AnalyzeExpense",
        "textract:AnalyzeID",
        "textract:StartDocumentAnalysis",
        "textract:StartExpenseAnalysis",
        "textract:GetDocumentAnalysis",
```

```
        "textract:GetExpenseAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Rekognition",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectLabels",
        "rekognition:DetectText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Comprehend",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:BatchDetectEntities",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectPiiEntities",
        "comprehend:DetectEntities",
        "comprehend:DetectSentiment",
        "comprehend:DetectDominantLanguage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:TagResource"
```

```
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker",
            "Canvas"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:RequestTag/Canvas" : "true",
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
      "Sid" : "GetStopAndDeleteBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetCustomModel",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:StopModelCustomizationJob",
        "bedrock:DeleteProvisionedModelThroughput"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "FoundationModelPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "BedrockFineTuningPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerCanvasBedrockAccess

描述：此政策透過提供 S3 等下游服務的存取權，授予在 SageMaker Canvas 中使用 Amazon Bedrock 的許可。

AmazonSageMakerCanvasBedrockAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerCanvasBedrockAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 2 月 2 日 18：37 UTC
- 編輯時間：2024 年 2 月 2 日 18：37 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerCanvasDataPrepFullAccess

描述：提供 Amazon SageMaker 資源和操作的完整存取權，以便在 Canvas 中進行資料準備。此政策也提供相關服務的選取存取權（例如 S3、IAM、KMS、RDS、CloudWatch Logs、Redshift、Athena、Glue、EventBridge、Secrets Manager)。此政策應連接至 Amazon SageMaker 網域/使用者設定檔執行角色。

`AmazonSageMakerCanvasDataPrepFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerCanvasDataPrepFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 10 月 27 日，UTC 22：56
- 編輯時間：2024 年 8 月 16 日 18：11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:*"
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
```

```
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerCanvasDirectDeployAccess

描述：允許 Amazon SageMaker Canvas 建立、管理和檢視透過 Canvas 建立之端點的端點詳細資訊。允許 Amazon SageMaker Canvas 從 CloudWatch 擷取端點調用指標。

`AmazonSageMakerCanvasDirectDeployAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerCanvasDirectDeployAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 10 月 6 日 18：11 UTC
- 編輯時間：2023 年 10 月 6 日 18：11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy

描述：此政策針對 Amazon SageMaker Canvas 用於大型資料處理的服務，將許可授予 Amazon EMR Serverless，例如 S3。

`AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 7 月 27 日 00：35 UTC
- 編輯時間：2024 年 7 月 27 日 00：35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "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*"
      ],
      "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" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerCanvasForecastAccess

描述：此政策會授予搭配 Amazon Forecast 使用 SageMaker Canvas 所需的許可。

AmazonSageMakerCanvasForecastAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerCanvasForecastAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 8 月 24 日，UTC 20：04
- 編輯時間：2022 年 8 月 24 日，UTC 20：04

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerCanvasFullAccess

描述：提供 Amazon SageMaker Canvas 資源和操作的完整存取權。此政策也提供相關服務的選取存取權（例如 S3、IAM、VPC、ECR、CloudWatch Logs、Redshift、Secrets Manager 和 Forecast)。此政策應連接至 Amazon SageMaker 網域/使用者設定檔執行角色。

`AmazonSageMakerCanvasFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerCanvasFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 9 月 9 日 00：44 UTC
- 編輯時間：2024 年 8 月 16 日 04：35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

政策版本

政策版本： v11（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeAutoMLJob",
```

```
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "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" : "DescribeScalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "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"
        }
```

```
      }
    },
    {
      "Sid" : "AthenaOperation",
      "Action" : [
        "athena:ListTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueOperation",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTables"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuicksightOperation",
      "Action" : [
        "quicksight:ListNamespaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUseOfKeyInAccount",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Source" : "SageMakerCanvas",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
```

```
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerCanvasSMDataScienceAssistantAccess

描述：提供 Amazon SageMaker Canvas 使用 SageMaker 資料科學助理服務的許可。資料科學助理目前同時使用 Amazon SageMaker 和 Amazon Q Developer 來處理使用者提示。

`AmazonSageMakerCanvasSMDataScienceAssistantAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerCanvasSMDataScienceAssistantAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 4 日 14：06 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasSMDataScienceAssistantAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "SageMakerDataScienceAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-data-science-assistant:SendConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSageMakerClusterInstanceRolePolicy

描述：此政策會授予使用 Amazon SageMaker 叢集通常需要的許可。

AmazonSageMakerClusterInstanceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerClusterInstanceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 11 月 29 日 15：11 UTC
- 編輯時間：2023 年 11 月 29 日 15：11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSageMakerCoreServiceRolePolicy

描述：Amazon SageMaker Core Services 的服務連結角色受管政策

`AmazonSageMakerCoreServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 21 日 21：40 UTC
- 編輯時間：2020 年 12 月 21 日 21：40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerEdgeDeviceFleetPolicy

描述：提供 SageMaker Edge 使用預設雲端連線為客戶建立和管理裝置機群所需的許可。

AmazonSageMakerEdgeDeviceFleetPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerEdgeDeviceFleetPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 12 月 8 日 16：17 UTC
- 編輯時間：2020 年 12 月 8 日 16：17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerFeatureStoreAccess

描述：提供為 Amazon SageMaker FeatureStore 功能群組啟用離線存放區所需的許可。

`AmazonSageMakerFeatureStoreAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerFeatureStoreAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 1 日 16：24 UTC
- 編輯時間：2022 年 12 月 5 日 14：19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSageMakerFullAccess

描述：透過 AWS 管理主控台 和 SDK 提供 Amazon SageMaker 的完整存取權。也提供相關服務的選取存取權 （ 例如 S3、ECR、CloudWatch Logs)。

AmazonSageMakerFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 11 月 29 日 13：07 UTC

- **編輯時間**：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

政策版本

政策版本： v29 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:*:*:partner-app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*",
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowAddTagsForSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
      ]
    },
    {
      "Sid" : "AllowUseOfTrainingPlanResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateCluster",
        "sagemaker:UpdateCluster",
        "sagemaker:DescribeTrainingPlan"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
```

```
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
```

```
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
```

```
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
```

```
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
```

```
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
```

```
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
```

```
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
```

```
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
```

```
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerGeospatialExecutionRole

描述：此政策提供使用 SageMaker 地理空間時通常需要的服務存取權。

AmazonSageMakerGeospatialExecutionRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerGeospatialExecutionRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 11 月 30 日 10：08 UTC
- 編輯時間：2023 年 5 月 10 日 20：28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerGeospatialFullAccess

描述：此政策授予許可，允許透過 AWS 管理主控台 和 SDK 完整存取 Amazon SageMaker 地理空間。

AmazonSageMakerGeospatialFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerGeospatialFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 11 月 30 日 10：06 UTC
- 編輯時間：2022 年 11 月 30 日 10：06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerGroundTruthExecution

描述：提供執行 SageMaker GroundTruth Labeling 任務所需的 AWS 服務存取權

AmazonSageMakerGroundTruthExecution 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerGroundTruthExecution 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 7 月 9 日 19：30 UTC
- 編輯時間：2022 年 4 月 29 日，UTC 20：49
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerHyperPodGatedModelAccess

描述：此 Amazon 受管政策提供 SageMaker HyperPod 在 SageMaker Jumpstart 中存取門控模型的必要許可。它允許在 SageMaker Public Hub 中建立中樞內容的URLs。

`AmazonSageMakerHyperPodGatedModelAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerHyperPodGatedModelAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2026 年 1 月 17 日 01：04 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodGatedModelAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "CreatePresignedUrlAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateHubContentPresignedUrls"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:hub/SageMakerPublicHub",
        "arn:aws:sagemaker:*:*:hub-content/SageMakerPublicHub/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerHyperPodInferenceAccess

描述：此政策提供設定 SageMaker HyperPod 推論運算子所需的管理權限。它可讓推論運算子存取在 HyperPod 叢集上部署和管理推論工作負載所需的 AWS 聯網資源、Amazon S3、Amazon ECR、Amazon CloudWatch、 AWS Certificate Manager 和 SageMaker 資源

`AmazonSageMakerHyperPodInferenceAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerHyperPodInferenceAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2026 年 1 月 27 日 20：34 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerHyperPodInferenceAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteObjectsPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "s3:ExistingObjectTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "S3PutObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::hyperpod-tls*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "s3:RequestObjectTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "ECRAuthorization",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRRepositoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "EC2DescribeAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2NetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EKSClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "EKSAccessEntryPolicyAssociation",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyarn" : "arn:aws:eks::aws:cluster-access-policy/
AmazonSagemakerHyperpodInferenceMonitoringPolicy"
        }
      }
    },
    {
      "Sid" : "ELBListAndDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FSxAccess",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "CertificateImportPermission",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:ImportCertificate"
      ],
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CreatedBy"
        },
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceTag/CreatedBy" : "HyperPodInference",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CertificateDeletePermission",
      "Effect" : "Allow",
      "Action" : "acm:DeleteCertificate",
      "Resource" : "arn:aws:acm:*:*:certificate/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerHyperPodInference*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "CloudWatchMetricsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeClusterInference",
        "sagemaker:UpdateClusterInference",
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
```

```
        "arn:aws:sagemaker:*:*:endpointconfig/*",
        "arn:aws:sagemaker:*:*:cluster/*",
        "arn:aws:sagemaker:*:*:hub-content/*",
        "arn:aws:sagemaker:*:*:hub/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModel",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "HyperPodInference"
        }
      }
    },
    {
      "Sid" : "SageMakerTagging",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
```

```
            "CreateModel",
            "CreateEndpointConfig",
            "CreateEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerDeleteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteModel",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "HyperPodInference"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerHyperPodObservabilityAdminAccess

描述：此政策提供設定 SageMaker HyperPod 可觀測性所需的管理權限。它可讓您存取 Amazon Managed Prometheus、Amazon Managed Grafana 和 EKS 附加元件。此政策也包含透過 ServiceAccountTokens 在您帳戶中的所有 Amazon Managed Grafana 工作區中廣泛存取 Grafana HTTP API。

`AmazonSageMakerHyperPodObservabilityAdminAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerHyperPodObservabilityAdminAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 7 月 10 日 14：37 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodObservabilityAdminAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrometheusCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusTagsAccess",
      "Effect" : "Allow",
      "Action" : "aps:TagResource",
      "Resource" : [
        "arn:aws:aps:*:*:/workspaces",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:DescribeWorkspace"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*"
    },
    {
      "Sid" : "PrometheusListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "PrometheusAlertsRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateAlertManagerDefinition",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces"
      ],
      "Resource" : [
        "arn:aws:aps:*:*:workspace/*",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ]
    },
    {
      "Sid" : "PrometheusCreateRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : "aps:CreateRuleGroupsNamespace",
      "Resource" : "arn:aws:aps:*:*:rulegroupsnamespace/*/
HyperPodObservabilityNamespace",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaCreateWorkspaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaTagsAccess",
      "Effect" : "Allow",
      "Action" : "grafana:TagResource",
```

```
      "Resource" : "arn:aws:grafana:*:*:/workspaces",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaListAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:ListWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaServiceAccountAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:CreateWorkspaceApiKey",
        "grafana:CreateWorkspaceServiceAccount",
        "grafana:CreateWorkspaceServiceAccountToken",
        "grafana:ListWorkspaceServiceAccounts",
        "grafana:ListWorkspaceServiceAccountTokens",
        "grafana:DeleteWorkspaceServiceAccountToken"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces/*"
    },
    {
      "Sid" : "IAMGrafanaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityGrafanaAccess-*",
      "Condition" : {
```

```
        "StringLike" : {
          "iam:PassedToService" : [
            "grafana.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMEKSPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*"
      ]
    },
    {
      "Sid" : "HyperPodClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListClusters",
        "sagemaker:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-sagemaker-hyperpod-observability/*"
    },
    {
      "Sid" : "EKSAddonDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeAddonConfiguration",
        "eks:DescribeAddonVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonPodIdentityAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribePodIdentityAssociation",
        "eks:DeletePodIdentityAssociation",
        "eks:UpdatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSListDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAddons",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "EKSCreateAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "eks:CreateAddon",
        "eks:CreatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSTagsAccess",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:addon/*/*/*",
        "arn:aws:eks:*:*:podidentityassociation/*/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "SSOAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:CreateManagedApplicationInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerHyperPodServiceRolePolicy

描述：此政策會將 Amazon SageMaker HyperPod 的許可授予相關 AWS 服務，例如 Amazon EKS、Amazon CloudWatch 等。

`AmazonSageMakerHyperPodServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 9 月 6 日 17：04 UTC
- 編輯時間：2024 年 9 月 6 日 17：04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerHyperPodServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Sid" : "EKSClusterDescribePermissions",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogStreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerHyperPodTrainingOperatorAccess

描述：此政策提供設定 SageMaker HyperPod 訓練運算子所需的管理許可。它可讓您存取 Amazon SageMaker HyperPod 和 EKS 附加元件。此政策包含描述您帳戶中 SageMaker HyperPod 資源的許可。

`AmazonSageMakerHyperPodTrainingOperatorAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerHyperPodTrainingOperatorAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 19 日 17：04 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodTrainingOperatorAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Sid" : "AllowDescribeClusterNodeOnHyperPodClusters",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeClusterNode",
      "Resource" : "arn:aws:sagemaker:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerMechanicalTurkAccess

描述：提供針對任何 Workteam 建立 Amazon 增強版 AI FlowDefinition 資源的存取權。

AmazonSageMakerMechanicalTurkAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerMechanicalTurkAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 16：19 UTC
- 編輯時間：2019 年 12 月 3 日 16：19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerModelGovernanceUseAccess

描述：此 AWS 受管政策會授予使用所有 Amazon SageMaker 控管功能所需的許可。此政策也提供相關服務的選取存取權 （例如 S3、KMS)。

AmazonSageMakerModelGovernanceUseAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerModelGovernanceUseAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 30 日 08：58 UTC
- 編輯時間：2024 年 6 月 4 日 21：48 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSMMonitoringModelCards",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker:DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:ListModelCardExportJobs"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSMTrainingModelsSearchTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListModels",
        "sagemaker:DescribeModel",
        "sagemaker:Search",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "sagemaker:ListTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3Actions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:CreateBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowS3ListActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSageMakerModelRegistryFullAccess

描述：這是 Sagemaker 中模型登錄檔的新受管政策。此政策是獨立的政策，可以連接到使用者角色，以存取 Sagemaker 中的模型登錄檔相關功能。

`AmazonSageMakerModelRegistryFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerModelRegistryFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 4 月 13 日 05：20 UTC
- 編輯時間：2024 年 6 月 6 日 18：48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:UpdateModelPackage"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryS3GetPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryS3ListPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryTagReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "sagemaker:collection"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:collection" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSageMakerNotebooksServiceRolePolicy

描述：Amazon SageMaker 筆記本的服務連結角色受管政策

AmazonSageMakerNotebooksServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 10 月 18 日 20：27 UTC
- 編輯時間：2025 年 12 月 10 日 18：34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFSxDescribe",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDeleteApp",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*"
    },
    {
      "Sid" : "AllowEFSAccessPointCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSAccessPointDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSMountWithDeletion",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEFSTagging",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEC2Tagging",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
```

```
    },
    {
      "Sid" : "AllowEC2Operations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2AuthZ",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowIdcOperations",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSagemakerProfileCreation",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowSagemakerSpaceOperationsForCanvasManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DescribeSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*"
    },
    {
      "Sid" : "AllowSagemakerAddTagsForAppManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerPartnerAppsFullAccess

描述：讓 Amazon SageMaker 合作夥伴應用程式使用者存取應用程式、列出可用的應用程式、啟動應用程式 Web UIs，以及透過應用程式 SDK 進行連線。

`AmazonSageMakerPartnerAppsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerPartnerAppsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 1 月 17 日 18：37 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerPartnerListAppsPermission",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListPartnerApps",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerPartnerAppsPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:DescribePartnerApp",
        "sagemaker:CallPartnerAppApi"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:sagemaker:*:*:partner-app/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

描述： AWS APIGateway 從 Amazon SageMaker 產品組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。授予一組相關服務的許可，包括 Lambda 和其他服務。

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以
將 AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 8 月 1 日 15：06 UTC
- 編輯時間：2023 年 8 月 1 日 15：06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServi

描述： AWS CloudFormation 從 Amazon SageMaker 產品組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。將許可授予相關服務的子集，包括 Lambda、APIGateway 等。

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以
將 `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 8 月 1 日 15：06 UTC
- 編輯時間：2023 年 8 月 1 日 15：06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

描述： AWS Lambda 從 Amazon SageMaker 產品組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。授予一組相關服務的許可，包括 Secrets Manager 和其他服務。

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以
將 AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 8 月 1 日 15：05 UTC
- 編輯時間：2023 年 8 月 1 日 15：05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerPipelinesIntegrations

描述：此 Amazon 受管政策授予與 SageMaker 模型建置管道中的回呼步驟和 Lambda 步驟搭配使用的常用許可。它會新增至可在設定 SageMaker Studio 時建立的 AmazonSageMaker-ExecutionRole。SageMaker 它也可以連接到將用於撰寫或執行管道的任何其他角色。

`AmazonSageMakerPipelinesIntegrations` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerPipelinesIntegrations` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 7 月 30 日 16：35 UTC
- 編輯時間：2023 年 2 月 17 日 21：28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerQuickSightVPCPolicy

描述：SageMaker Unified Studios 將使用此政策為 QuickSight 建立 VPC 相關資源

`AmazonSageMakerQuickSightVPCPolicy` 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerQuickSightVPCPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 6 月 3 日 17：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerQuickSightVPCPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageQuickSightVPCConnection",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListVPCConnections",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcconnection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DescribeQuickSightVPCConnectionEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightEC2NetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSageMakerReadOnly

描述：透過 AWS 管理主控台 和 SDK 提供 Amazon SageMaker 的唯讀存取權。

AmazonSageMakerReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 29 日 13：07 UTC
- 編輯時間：2021 年 12 月 1 日 16：29 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerReadOnly

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

描述： AWS APIGateway 從 Amazon SageMaker 產品組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。授予一組相關服務的許可，包括 CloudWatch Logs 和其他服務。

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 3 月 25 日 04：25 UTC
- 編輯時間：2022 年 3 月 25 日 04：25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

描述： AWS CloudFormation 從 Amazon SageMaker 產品組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。將許可授予相關服務的子集，包括 SageMaker 和其他服務。

AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以
將 AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 3 月 25 日 04：26 UTC
- 編輯時間：2022 年 3 月 25 日 04：26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

描述： AWS CodeBuild 從 Amazon SageMaker 產品組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。將許可授予相關服務的子集，包括 CodePipeline、CodeBuild 等。

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 3 月 25 日 04：27 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
```

```
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildPassRoletPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildLogPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
```

```
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
```

```
            "sagemaker:CreateFlowDefinition",
            "sagemaker:CreateHumanTaskUi",
            "sagemaker:CreateHyperParameterTuningJob",
            "sagemaker:CreateImage",
            "sagemaker:CreateImageVersion",
            "sagemaker:CreateInferenceRecommendationsJob",
            "sagemaker:CreateLabelingJob",
            "sagemaker:CreateLineageGroupPolicy",
            "sagemaker:CreateModel",
            "sagemaker:CreateModelBiasJobDefinition",
            "sagemaker:CreateModelExplainabilityJobDefinition",
            "sagemaker:CreateModelPackage",
            "sagemaker:CreateModelPackageGroup",
            "sagemaker:CreateModelQualityJobDefinition",
            "sagemaker:CreateMonitoringSchedule",
            "sagemaker:CreateNotebookInstance",
            "sagemaker:CreateNotebookInstanceLifecycleConfig",
            "sagemaker:CreatePipeline",
            "sagemaker:CreatePresignedDomainUrl",
            "sagemaker:CreatePresignedNotebookInstanceUrl",
            "sagemaker:CreateProcessingJob",
            "sagemaker:CreateProject",
            "sagemaker:CreateTrainingJob",
            "sagemaker:CreateTransformJob",
            "sagemaker:CreateTrial",
            "sagemaker:CreateTrialComponent",
            "sagemaker:CreateUserProfile",
            "sagemaker:CreateWorkforce",
            "sagemaker:CreateWorkteam",
            "sagemaker:DeleteAction",
            "sagemaker:DeleteAlgorithm",
            "sagemaker:DeleteApp",
            "sagemaker:DeleteAppImageConfig",
            "sagemaker:DeleteArtifact",
            "sagemaker:DeleteAssociation",
            "sagemaker:DeleteCodeRepository",
            "sagemaker:DeleteContext",
            "sagemaker:DeleteDataQualityJobDefinition",
            "sagemaker:DeleteDeviceFleet",
            "sagemaker:DeleteDomain",
            "sagemaker:DeleteEndpoint",
            "sagemaker:DeleteEndpointConfig",
            "sagemaker:DeleteExperiment",
            "sagemaker:DeleteFeatureGroup",
```

```
            "sagemaker:DeleteFlowDefinition",
            "sagemaker:DeleteHumanLoop",
            "sagemaker:DeleteHumanTaskUi",
            "sagemaker:DeleteImage",
            "sagemaker:DeleteImageVersion",
            "sagemaker:DeleteLineageGroupPolicy",
            "sagemaker:DeleteModel",
            "sagemaker:DeleteModelBiasJobDefinition",
            "sagemaker:DeleteModelExplainabilityJobDefinition",
            "sagemaker:DeleteModelPackage",
            "sagemaker:DeleteModelPackageGroup",
            "sagemaker:DeleteModelPackageGroupPolicy",
            "sagemaker:DeleteModelQualityJobDefinition",
            "sagemaker:DeleteMonitoringSchedule",
            "sagemaker:DeleteNotebookInstance",
            "sagemaker:DeleteNotebookInstanceLifecycleConfig",
            "sagemaker:DeletePipeline",
            "sagemaker:DeleteProject",
            "sagemaker:DeleteRecord",
            "sagemaker:DeleteTags",
            "sagemaker:DeleteTrial",
            "sagemaker:DeleteTrialComponent",
            "sagemaker:DeleteUserProfile",
            "sagemaker:DeleteWorkforce",
            "sagemaker:DeleteWorkteam",
            "sagemaker:DeregisterDevices",
            "sagemaker:DescribeAction",
            "sagemaker:DescribeAlgorithm",
            "sagemaker:DescribeApp",
            "sagemaker:DescribeAppImageConfig",
            "sagemaker:DescribeArtifact",
            "sagemaker:DescribeAutoMLJob",
            "sagemaker:DescribeCodeRepository",
            "sagemaker:DescribeCompilationJob",
            "sagemaker:DescribeContext",
            "sagemaker:DescribeDataQualityJobDefinition",
            "sagemaker:DescribeDevice",
            "sagemaker:DescribeDeviceFleet",
            "sagemaker:DescribeDomain",
            "sagemaker:DescribeEdgePackagingJob",
            "sagemaker:DescribeEndpoint",
            "sagemaker:DescribeEndpointConfig",
            "sagemaker:DescribeExperiment",
            "sagemaker:DescribeFeatureGroup",
```

```
            "sagemaker:DescribeFlowDefinition",
            "sagemaker:DescribeHumanLoop",
            "sagemaker:DescribeHumanTaskUi",
            "sagemaker:DescribeHyperParameterTuningJob",
            "sagemaker:DescribeImage",
            "sagemaker:DescribeImageVersion",
            "sagemaker:DescribeInferenceRecommendationsJob",
            "sagemaker:DescribeLabelingJob",
            "sagemaker:DescribeLineageGroup",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeModelBiasJobDefinition",
            "sagemaker:DescribeModelExplainabilityJobDefinition",
            "sagemaker:DescribeModelPackage",
            "sagemaker:DescribeModelPackageGroup",
            "sagemaker:DescribeModelQualityJobDefinition",
            "sagemaker:DescribeMonitoringSchedule",
            "sagemaker:DescribeNotebookInstance",
            "sagemaker:DescribeNotebookInstanceLifecycleConfig",
            "sagemaker:DescribePipeline",
            "sagemaker:DescribePipelineDefinitionForExecution",
            "sagemaker:DescribePipelineExecution",
            "sagemaker:DescribeProcessingJob",
            "sagemaker:DescribeProject",
            "sagemaker:DescribeSubscribedWorkteam",
            "sagemaker:DescribeTrainingJob",
            "sagemaker:DescribeTransformJob",
            "sagemaker:DescribeTrial",
            "sagemaker:DescribeTrialComponent",
            "sagemaker:DescribeUserProfile",
            "sagemaker:DescribeWorkforce",
            "sagemaker:DescribeWorkteam",
            "sagemaker:DisableSagemakerServicecatalogPortfolio",
            "sagemaker:DisassociateTrialComponent",
            "sagemaker:EnableSagemakerServicecatalogPortfolio",
            "sagemaker:GetDeviceFleetReport",
            "sagemaker:GetDeviceRegistration",
            "sagemaker:GetLineageGroupPolicy",
            "sagemaker:GetModelPackageGroupPolicy",
            "sagemaker:GetRecord",
            "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
            "sagemaker:GetSearchSuggestions",
            "sagemaker:InvokeEndpoint",
            "sagemaker:InvokeEndpointAsync",
            "sagemaker:ListActions",
```

```
            "sagemaker:ListAlgorithms",
            "sagemaker:ListAppImageConfigs",
            "sagemaker:ListApps",
            "sagemaker:ListArtifacts",
            "sagemaker:ListAssociations",
            "sagemaker:ListAutoMLJobs",
            "sagemaker:ListCandidatesForAutoMLJob",
            "sagemaker:ListCodeRepositories",
            "sagemaker:ListCompilationJobs",
            "sagemaker:ListContexts",
            "sagemaker:ListDataQualityJobDefinitions",
            "sagemaker:ListDeviceFleets",
            "sagemaker:ListDevices",
            "sagemaker:ListDomains",
            "sagemaker:ListEdgePackagingJobs",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListEndpoints",
            "sagemaker:ListExperiments",
            "sagemaker:ListFeatureGroups",
            "sagemaker:ListFlowDefinitions",
            "sagemaker:ListHumanLoops",
            "sagemaker:ListHumanTaskUis",
            "sagemaker:ListHyperParameterTuningJobs",
            "sagemaker:ListImageVersions",
            "sagemaker:ListImages",
            "sagemaker:ListInferenceRecommendationsJobs",
            "sagemaker:ListLabelingJobs",
            "sagemaker:ListLabelingJobsForWorkteam",
            "sagemaker:ListLineageGroups",
            "sagemaker:ListModelBiasJobDefinitions",
            "sagemaker:ListModelExplainabilityJobDefinitions",
            "sagemaker:ListModelMetadata",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelPackages",
            "sagemaker:ListModelQualityJobDefinitions",
            "sagemaker:ListModels",
            "sagemaker:ListMonitoringExecutions",
            "sagemaker:ListMonitoringSchedules",
            "sagemaker:ListNotebookInstanceLifecycleConfigs",
            "sagemaker:ListNotebookInstances",
            "sagemaker:ListPipelineExecutionSteps",
            "sagemaker:ListPipelineExecutions",
            "sagemaker:ListPipelineParametersForExecution",
            "sagemaker:ListPipelines",
```

```
            "sagemaker:ListProcessingJobs",
            "sagemaker:ListProjects",
            "sagemaker:ListSubscribedWorkteams",
            "sagemaker:ListTags",
            "sagemaker:ListTrainingJobs",
            "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
            "sagemaker:ListTransformJobs",
            "sagemaker:ListTrialComponents",
            "sagemaker:ListTrials",
            "sagemaker:ListUserProfiles",
            "sagemaker:ListWorkforces",
            "sagemaker:ListWorkteams",
            "sagemaker:PutLineageGroupPolicy",
            "sagemaker:PutModelPackageGroupPolicy",
            "sagemaker:PutRecord",
            "sagemaker:QueryLineage",
            "sagemaker:RegisterDevices",
            "sagemaker:RenderUiTemplate",
            "sagemaker:Search",
            "sagemaker:SendHeartbeat",
            "sagemaker:SendPipelineExecutionStepFailure",
            "sagemaker:SendPipelineExecutionStepSuccess",
            "sagemaker:StartHumanLoop",
            "sagemaker:StartMonitoringSchedule",
            "sagemaker:StartNotebookInstance",
            "sagemaker:StartPipelineExecution",
            "sagemaker:StopAutoMLJob",
            "sagemaker:StopCompilationJob",
            "sagemaker:StopEdgePackagingJob",
            "sagemaker:StopHumanLoop",
            "sagemaker:StopHyperParameterTuningJob",
            "sagemaker:StopInferenceRecommendationsJob",
            "sagemaker:StopLabelingJob",
            "sagemaker:StopMonitoringSchedule",
            "sagemaker:StopNotebookInstance",
            "sagemaker:StopPipelineExecution",
            "sagemaker:StopProcessingJob",
            "sagemaker:StopTrainingJob",
            "sagemaker:StopTransformJob",
            "sagemaker:UpdateAction",
            "sagemaker:UpdateAppImageConfig",
            "sagemaker:UpdateArtifact",
            "sagemaker:UpdateCodeRepository",
            "sagemaker:UpdateContext",
```

```
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

描述： AWS CodePipeline 從 Amazon SageMaker 產品組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。將許可授予相關服務的子集，包括 CodePipeline、CodeBuild 等。

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以
將 AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 2 月 22 日 09：53 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
```

```
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
```

```
      "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
```

```
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

描述： AWS ServiceCatalog 佈建產品中 AWS CloudWatch Events 從 Amazon SageMaker 產品組合中使用的服務角色政策。將許可授予相關服務的子集，包括 CodePipeline 和其他服務。

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 2 月 22 日 09：53 UTC

- **編輯時間**：2022 年 2 月 22 日 09：53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

描述： AWS Firehose 從 Amazon SageMaker 產品組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。授予一組相關服務的許可，包括 Firehose 和其他服務。

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 2 月 22 日 09：54 UTC
- 編輯時間：2022 年 2 月 22 日 09：54 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

描述： AWS ServiceCatalog AWS 佈建產品中 Glue 從 Amazon SageMaker 產品組合中使用的服務角色政策。授予一組相關服務的許可，包括 Glue、S3 和其他服務。

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 2 月 22 日 09：51 UTC
- 編輯時間：2022 年 8 月 26 日 19：13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

描述： AWS Lambda 從 Amazon SageMaker 產品組合的 AWS ServiceCatalog 佈建產品中使用的服務角色政策。將許可授予一組相關服務，包括 ECR、S3 和其他服務。

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 4 月 4 日 16：34 UTC
- 編輯時間：2024 年 6 月 11 日 18：57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerLambdaECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
```

```
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
```

```
            "sagemaker:CreateCodeRepository",
            "sagemaker:CreateCompilationJob",
            "sagemaker:CreateContext",
            "sagemaker:CreateDataQualityJobDefinition",
            "sagemaker:CreateDeviceFleet",
            "sagemaker:CreateDomain",
            "sagemaker:CreateEdgePackagingJob",
            "sagemaker:CreateEndpoint",
            "sagemaker:CreateEndpointConfig",
            "sagemaker:CreateExperiment",
            "sagemaker:CreateFeatureGroup",
            "sagemaker:CreateFlowDefinition",
            "sagemaker:CreateHumanTaskUi",
            "sagemaker:CreateHyperParameterTuningJob",
            "sagemaker:CreateImage",
            "sagemaker:CreateImageVersion",
            "sagemaker:CreateInferenceRecommendationsJob",
            "sagemaker:CreateLabelingJob",
            "sagemaker:CreateLineageGroupPolicy",
            "sagemaker:CreateModel",
            "sagemaker:CreateModelBiasJobDefinition",
            "sagemaker:CreateModelExplainabilityJobDefinition",
            "sagemaker:CreateModelPackage",
            "sagemaker:CreateModelPackageGroup",
            "sagemaker:CreateModelQualityJobDefinition",
            "sagemaker:CreateMonitoringSchedule",
            "sagemaker:CreateNotebookInstance",
            "sagemaker:CreateNotebookInstanceLifecycleConfig",
            "sagemaker:CreatePipeline",
            "sagemaker:CreatePresignedDomainUrl",
            "sagemaker:CreatePresignedNotebookInstanceUrl",
            "sagemaker:CreateProcessingJob",
            "sagemaker:CreateProject",
            "sagemaker:CreateTrainingJob",
            "sagemaker:CreateTransformJob",
            "sagemaker:CreateTrial",
            "sagemaker:CreateTrialComponent",
            "sagemaker:CreateUserProfile",
            "sagemaker:CreateWorkforce",
            "sagemaker:CreateWorkteam",
            "sagemaker:DeleteAction",
            "sagemaker:DeleteAlgorithm",
            "sagemaker:DeleteApp",
            "sagemaker:DeleteAppImageConfig",
```

```
            "sagemaker:DeleteArtifact",
            "sagemaker:DeleteAssociation",
            "sagemaker:DeleteCodeRepository",
            "sagemaker:DeleteContext",
            "sagemaker:DeleteDataQualityJobDefinition",
            "sagemaker:DeleteDeviceFleet",
            "sagemaker:DeleteDomain",
            "sagemaker:DeleteEndpoint",
            "sagemaker:DeleteEndpointConfig",
            "sagemaker:DeleteExperiment",
            "sagemaker:DeleteFeatureGroup",
            "sagemaker:DeleteFlowDefinition",
            "sagemaker:DeleteHumanLoop",
            "sagemaker:DeleteHumanTaskUi",
            "sagemaker:DeleteImage",
            "sagemaker:DeleteImageVersion",
            "sagemaker:DeleteLineageGroupPolicy",
            "sagemaker:DeleteModel",
            "sagemaker:DeleteModelBiasJobDefinition",
            "sagemaker:DeleteModelExplainabilityJobDefinition",
            "sagemaker:DeleteModelPackage",
            "sagemaker:DeleteModelPackageGroup",
            "sagemaker:DeleteModelPackageGroupPolicy",
            "sagemaker:DeleteModelQualityJobDefinition",
            "sagemaker:DeleteMonitoringSchedule",
            "sagemaker:DeleteNotebookInstance",
            "sagemaker:DeleteNotebookInstanceLifecycleConfig",
            "sagemaker:DeletePipeline",
            "sagemaker:DeleteProject",
            "sagemaker:DeleteRecord",
            "sagemaker:DeleteTags",
            "sagemaker:DeleteTrial",
            "sagemaker:DeleteTrialComponent",
            "sagemaker:DeleteUserProfile",
            "sagemaker:DeleteWorkforce",
            "sagemaker:DeleteWorkteam",
            "sagemaker:DeregisterDevices",
            "sagemaker:DescribeAction",
            "sagemaker:DescribeAlgorithm",
            "sagemaker:DescribeApp",
            "sagemaker:DescribeAppImageConfig",
            "sagemaker:DescribeArtifact",
            "sagemaker:DescribeAutoMLJob",
            "sagemaker:DescribeCodeRepository",
```

```
            "sagemaker:DescribeCompilationJob",
            "sagemaker:DescribeContext",
            "sagemaker:DescribeDataQualityJobDefinition",
            "sagemaker:DescribeDevice",
            "sagemaker:DescribeDeviceFleet",
            "sagemaker:DescribeDomain",
            "sagemaker:DescribeEdgePackagingJob",
            "sagemaker:DescribeEndpoint",
            "sagemaker:DescribeEndpointConfig",
            "sagemaker:DescribeExperiment",
            "sagemaker:DescribeFeatureGroup",
            "sagemaker:DescribeFlowDefinition",
            "sagemaker:DescribeHumanLoop",
            "sagemaker:DescribeHumanTaskUi",
            "sagemaker:DescribeHyperParameterTuningJob",
            "sagemaker:DescribeImage",
            "sagemaker:DescribeImageVersion",
            "sagemaker:DescribeInferenceRecommendationsJob",
            "sagemaker:DescribeLabelingJob",
            "sagemaker:DescribeLineageGroup",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeModelBiasJobDefinition",
            "sagemaker:DescribeModelExplainabilityJobDefinition",
            "sagemaker:DescribeModelPackage",
            "sagemaker:DescribeModelPackageGroup",
            "sagemaker:DescribeModelQualityJobDefinition",
            "sagemaker:DescribeMonitoringSchedule",
            "sagemaker:DescribeNotebookInstance",
            "sagemaker:DescribeNotebookInstanceLifecycleConfig",
            "sagemaker:DescribePipeline",
            "sagemaker:DescribePipelineDefinitionForExecution",
            "sagemaker:DescribePipelineExecution",
            "sagemaker:DescribeProcessingJob",
            "sagemaker:DescribeProject",
            "sagemaker:DescribeSubscribedWorkteam",
            "sagemaker:DescribeTrainingJob",
            "sagemaker:DescribeTransformJob",
            "sagemaker:DescribeTrial",
            "sagemaker:DescribeTrialComponent",
            "sagemaker:DescribeUserProfile",
            "sagemaker:DescribeWorkforce",
            "sagemaker:DescribeWorkteam",
            "sagemaker:DisableSagemakerServicecatalogPortfolio",
            "sagemaker:DisassociateTrialComponent",
```

```
            "sagemaker:EnableSagemakerServicecatalogPortfolio",
            "sagemaker:GetDeviceFleetReport",
            "sagemaker:GetDeviceRegistration",
            "sagemaker:GetLineageGroupPolicy",
            "sagemaker:GetModelPackageGroupPolicy",
            "sagemaker:GetRecord",
            "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
            "sagemaker:GetSearchSuggestions",
            "sagemaker:InvokeEndpoint",
            "sagemaker:InvokeEndpointAsync",
            "sagemaker:ListActions",
            "sagemaker:ListAlgorithms",
            "sagemaker:ListAppImageConfigs",
            "sagemaker:ListApps",
            "sagemaker:ListArtifacts",
            "sagemaker:ListAssociations",
            "sagemaker:ListAutoMLJobs",
            "sagemaker:ListCandidatesForAutoMLJob",
            "sagemaker:ListCodeRepositories",
            "sagemaker:ListCompilationJobs",
            "sagemaker:ListContexts",
            "sagemaker:ListDataQualityJobDefinitions",
            "sagemaker:ListDeviceFleets",
            "sagemaker:ListDevices",
            "sagemaker:ListDomains",
            "sagemaker:ListEdgePackagingJobs",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListEndpoints",
            "sagemaker:ListExperiments",
            "sagemaker:ListFeatureGroups",
            "sagemaker:ListFlowDefinitions",
            "sagemaker:ListHumanLoops",
            "sagemaker:ListHumanTaskUis",
            "sagemaker:ListHyperParameterTuningJobs",
            "sagemaker:ListImageVersions",
            "sagemaker:ListImages",
            "sagemaker:ListInferenceRecommendationsJobs",
            "sagemaker:ListLabelingJobs",
            "sagemaker:ListLabelingJobsForWorkteam",
            "sagemaker:ListLineageGroups",
            "sagemaker:ListModelBiasJobDefinitions",
            "sagemaker:ListModelExplainabilityJobDefinitions",
            "sagemaker:ListModelMetadata",
            "sagemaker:ListModelPackageGroups",
```

```
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
```

```
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:algorithm/*",
        "arn:aws:sagemaker:*:*:app-image-config/*",
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:automl-job/*",
        "arn:aws:sagemaker:*:*:code-repository/*",
        "arn:aws:sagemaker:*:*:compilation-job/*",
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
        "arn:aws:sagemaker:*:*:device-fleet/*",
```

```
        "arn:aws:sagemaker:*:*:edge-packaging-job/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:experiment/*",
        "arn:aws:sagemaker:*:*:experiment-trial/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:feature-group/*",
        "arn:aws:sagemaker:*:*:human-loop/*",
        "arn:aws:sagemaker:*:*:human-task-ui/*",
        "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
        "arn:aws:sagemaker:*:*:image/*",
        "arn:aws:sagemaker:*:*:image-version/*/*",
        "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
        "arn:aws:sagemaker:*:*:labeling-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
        "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:monitoring-schedule/*",
        "arn:aws:sagemaker:*:*:notebook-instance/*",
        "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    },
```

```
    {
      "Sid" : "AmazonSageMakerLambdaLogPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Sid" : "AmazonSageMakerLambdaCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/sagemaker-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:project-name" : "*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerSpacesControllerPolicy

描述：授予 SageMaker Spaces 附加元件所需的 Systems Manager 啟用、工作階段管理和 KMS 金鑰操作許可，以啟用對 EKS SageMaker Spaces 的安全遠端存取。

`AmazonSageMakerSpacesControllerPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerSpacesControllerPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 19 日 04：34 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesControllerPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "AllowOperatorToSSMCreateActivationForSpaces",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeActivations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeActivations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeSessions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeleteActivation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToActivation",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:iam::*:role/sagemaker-space-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeManagedNodes",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeregisterWorkspaceInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToPassSsmManagedNodeRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/sagemaker-space-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowStartSessionDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-StartSSHSession",
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "AllowOperatorToSSMCreateDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToEnableAdvancedTierForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting",
        "ssm:ResetServiceSetting"
      ],
```

```
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/activation-
tier"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToSSMDocument",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerSpacesRouterPolicy

描述：授予 SageMaker Spaces 路由器所需的 Systems KMS 金鑰操作許可，以啟用對 EKS SageMaker Spaces 的安全遠端存取。

AmazonSageMakerSpacesRouterPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonSageMakerSpacesRouterPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 19 日 04：34 UTC

- **編輯時間**：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesRouterPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSageMakerTrainingPlanCreateAccess

描述：此 Amazon 受管政策提供建立和管理 SageMaker Training Plans 的必要許可。它允許使用者建立 Training Plans 和預留容量、描述現有的 Training Plans，以及執行搜尋和清單操作。

`AmazonSageMakerTrainingPlanCreateAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSageMakerTrainingPlanCreateAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 4 日 13：21 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerTrainingPlanCreateAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "CreateTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingPlan",
        "sagemaker:CreateReservedCapacity",
        "sagemaker:DescribeReservedCapacity"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AddTagsToTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateTrainingPlan",
            "CreateReservedCapacity"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeTrainingPlan",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*"
      ]
    },
    {
      "Sid" : "NonResourceLevelTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SearchTrainingPlanOfferings",
```

```
        "sagemaker:ListTrainingPlans"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListUltraServersByReservedCapacityPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListUltraServersByReservedCapacity",
      "Resource" : [
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSecurityLakeAdministrator

描述：提供 Amazon Security Lake 的完整存取權，以及管理 Security Lake 所需的相關服務。

`AmazonSecurityLakeAdministrator` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSecurityLakeAdministrator` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 5 月 30 日 22：04 UTC
- 編輯時間：2024 年 2 月 23 日 16：01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "AllowRolePolicyActionsforSubscibersandSources",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowRegisterS3LocationInLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PutRolePolicy",
        "iam:GetRolePolicy"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowIAMActionsByResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRolePolicies",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakes",
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
    },
    {
      "Sid" : "S3ResourcelessReadOnly",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSecurityLakeMetastoreManager

描述：Amazon SecurityLake 中繼存放區管理員 lambda 的政策，允許存取 cloudwatch、S3、Glue 和 SQS。

`AmazonSecurityLakeMetastoreManager` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSecurityLakeMetastoreManager` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2024 年 1 月 23 日 15：26 UTC
- 編輯時間：2024 年 4 月 1 日 20：04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGlueManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToReadFromSqs",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataReadWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCleanup",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSecurityLakePermissionsBoundary

描述：Amazon Security Lake 會為第三方自訂來源建立 IAM 角色，以將資料寫入資料湖，並為第三方訂閱者建立從資料湖取用資料，並在建立這些角色時使用此政策來定義其許可界限。

`AmazonSecurityLakePermissionsBoundary` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSecurityLakePermissionsBoundary` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 29 日 14：11 UTC
- 編輯時間：2024 年 5 月 14 日，UTC 20：39

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

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsForSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsForSecurityLake",
      "Effect" : "Deny",
      "NotAction" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
```

```
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeBucket",
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeSQS",
      "Effect" : "Deny",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
```

```
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sqs:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:sqs:arn" : [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSESFullAccess

描述：透過 提供 Amazon SES 的完整存取權 AWS 管理主控台。

`AmazonSESFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSESFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSESReadOnlyAccess

描述：透過 提供 Amazon SES 的唯讀存取權 AWS 管理主控台。

AmazonSESReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSESReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2024 年 5 月 14 日 12：03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSESServiceRolePolicy

描述：允許 SES 代表您的 SES 資源發佈 Amazon CloudWatch 基本監控指標

AmazonSESServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 5 月 21 日 16：02 UTC
- 編輯時間：2024 年 5 月 21 日 16：02 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricDataToSESCloudWatchNamespaces",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "AWS/SES",
```

```
            "AWS/SES/MailManager",
            "AWS/SES/Addons"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSNSFullAccess

描述：透過 提供 Amazon SNS 的完整存取權 AWS 管理主控台。

AmazonSNSFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSNSFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2024 年 9 月 24 日，UTC 22：32
- ARN: arn:aws:iam::aws:policy/AmazonSNSFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSFullAccess",
      "Effect" : "Allow",
      "Action" : "sns:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:CreateVerifiedDestinationNumber",
        "sms-voice:SendDestinationNumberVerificationCode",
        "sms-voice:SendTextMessage",
        "sms-voice:DeleteVerifiedDestinationNumber",
        "sms-voice:VerifyDestinationNumber",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:SetTextMessageSpendLimitOverride",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DeleteOptedOutNumber"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSNSReadOnlyAccess

描述：透過 提供 Amazon SNS 的唯讀存取權 AWS 管理主控台。

AmazonSNSReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSNSReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2024 年 9 月 24 日，UTC 22：13
- ARN: arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:List*",
```

```
        "sns:CheckIfPhoneNumberIsOptedOut",
        "sns:GetEndpointAttributes",
        "sns:GetDataProtectionPolicy",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetSMSAttributes",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribeOptedOutNumbers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSNSRole

描述：Amazon SNS 服務角色的預設政策。

AmazonSNSRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonSNSRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSNSRole

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSQSFullAccess

描述：透過 提供 Amazon SQS 的完整存取權 AWS 管理主控台。

AmazonSQSFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSQSFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSQSFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Action" : [
        "sqs:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSQSReadOnlyAccess

描述：透過 提供 Amazon SQS 的唯讀存取權 AWS 管理主控台。

`AmazonSQSReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSQSReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2024 年 5 月 24 日 18：16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSSMAutomationApproverAccess

描述：提供檢視自動化執行的存取權，並將核准決策傳送至等待核准的自動化

AmazonSSMAutomationApproverAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSSMAutomationApproverAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 8 月 7 日 23：07 UTC
- 編輯時間：2017 年 8 月 7 日 23：07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonSSMAutomationRole

描述：提供 EC2 Automation 服務執行自動化文件中定義之活動的許可

AmazonSSMAutomationRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonSSMAutomationRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 12 月 5 日，UTC 22：09
- 編輯時間：2026 年 3 月 20 日 17：42 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:Automation*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:session/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSSMDirectoryServiceAccess

描述：此政策允許 SSM Agent 代表客戶存取 Directory Service，以加入受管執行個體的網域。

`AmazonSSMDirectoryServiceAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSSMDirectoryServiceAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 3 月 15 日 17：44 UTC
- 編輯時間：2019 年 3 月 15 日 17：44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSSMFullAccess

描述：提供 Amazon SSM 的完整存取權。

AmazonSSMFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSSMFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 5 月 29 日 17：39 UTC
- 編輯時間：2019 年 11 月 20 日，UTC 20：08
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSSMMaintenanceWindowRole

描述：用於 EC2 維護時段的服務角色

AmazonSSMMaintenanceWindowRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonSSMMaintenanceWindowRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 12 月 1 日 15：57 UTC
- 編輯時間：2019 年 7 月 27 日 00：16 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:ListGroups",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSSMManagedEC2InstanceDefaultPolicy

描述：此政策會在 EC2 執行個體上啟用 AWS Systems Manager 功能。

AmazonSSMManagedEC2InstanceDefaultPolicy 是 AWS 受管政策。

使用此政策

您可以將 AmazonSSMManagedEC2InstanceDefaultPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 8 月 30 日，UTC 20：54
- 編輯時間：2024 年 7 月 16 日 18：14 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMAgentPermissions",
      "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" : "*"
    },
    {
      "Sid" : "AllowSSMChannelMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSMLegacyMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSSMManagedInstanceCore

描述：Amazon EC2 角色的政策，用於啟用 AWS Systems Manager 服務核心功能。

AmazonSSMManagedInstanceCore 是 AWS 受管政策。

使用此政策

您可以將 AmazonSSMManagedInstanceCore 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 3 月 15 日 17：22 UTC
- 編輯時間：2019 年 5 月 23 日 16：54 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSSMPatchAssociation

描述：為修補程式關聯操作提供子執行個體的存取權。

AmazonSSMPatchAssociation 是 AWS 受管政策。

使用此政策

您可以將 AmazonSSMPatchAssociation 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 5 月 13 日 16：00 UTC
- 編輯時間：2020 年 5 月 13 日 16：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonSSMPatchAssociation

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSSMReadOnlyAccess

描述：提供 Amazon SSM 的唯讀存取權。

`AmazonSSMReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonSSMReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 5 月 29 日 17：44 UTC
- 編輯時間：2015 年 5 月 29 日 17：44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonSSMServiceRolePolicy

描述：提供 Amazon SSM 管理或使用 AWS 的資源存取權

AmazonSSMServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 11 月 13 日 19：20 UTC
- 編輯時間：2025 年 7 月 15 日 17：22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy

政策版本

政策版本： v16 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:PutInventory"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "ssm:InventoryTypeName" : [
            "AWS:ComplianceItem",
            "AWS:PatchSummary"
          ]
        }
      }
    },
    {
      "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:ListGroups",
        "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" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-explorer-2:CreateManagedView",
      "Resource" : "arn:aws:resource-explorer-2:*:*:managed-view/AWSManagedViewForSSM*"
    }
  ]
```

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonSumerianFullAccess

描述：提供 Amazon Sumerian 的完整存取權。

AmazonSumerianFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonSumerianFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 4 月 24 日，UTC 20：14
- 編輯時間：2018 年 4 月 24 日，UTC 20：14
- ARN: arn:aws:iam::aws:policy/AmazonSumerianFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTextractFullAccess

描述：存取所有 Amazon Textract APIs

AmazonTextractFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonTextractFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 11 月 28 日 19：07 UTC
- 編輯時間：2018 年 11 月 28 日 19：07 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTextractFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTextractServiceRole

描述：允許 Textract 代表您呼叫 AWS 服務。

AmazonTextractServiceRole 是 AWS 受管政策。

使用此政策

您可以將 AmazonTextractServiceRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 11 月 28 日 19：12 UTC
- 編輯時間：2018 年 11 月 28 日 19：12 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTimestreamConsoleFullAccess

描述：提供使用 管理 Amazon Timestream 的完整存取權 AWS 管理主控台。請注意，此政策也會授予特定 KMS 操作的許可，以及管理已儲存查詢的操作。如果使用客戶受管 CMK，請參閱 文件以取得所需的其他許可。

`AmazonTimestreamConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonTimestreamConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 9 月 30 日，UTC 21：47
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "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" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:ListEntitlementDetails",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:Subscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-5jijo74ujy36m",
            "prod-rjppt7huo35fm"
          ]
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTimestreamFullAccess

描述：提供 Amazon Timestream 的完整存取權。請注意，此政策也會授予特定 KMS 操作存取權。如果使用客戶受管 CMK，請參閱 文件以取得所需的其他許可。

`AmazonTimestreamFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonTimestreamFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 9 月 30 日，UTC 21：47
- 編輯時間：2021 年 11 月 26 日 23：42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTimestreamInfluxDBFullAccess

描述：提供建立、更新、刪除和列出 Amazon Timestream InfluxDB 執行個體，以及建立和列出參數群組的完整管理存取權。如需其他所需許可，請參閱 文件。

`AmazonTimestreamInfluxDBFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonTimestreamInfluxDBFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 3 月 14 日 22：53 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

政策版本

政策版本： v17 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster"
      ],
      "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",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "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:::*"
      ]
    },
    {
      "Sid" : "MPViewAccessStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MPSubscriptionAccessStatement",
      "Effect" : "Allow",
      "Action" : "aws-marketplace:Subscribe",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

描述：提供管理存取權來管理 Amazon Timestream InfluxDB 執行個體和參數群組，但市集操作除外。

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 4 月 17 日 17：52 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
```

```
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster"
      ],
      "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",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "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:::*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTimestreamInfluxDBServiceRolePolicy

描述：提供建立、更新、刪除和列出 Amazon Timestream InfluxDB 執行個體，以及建立和列出參數群組的完整管理存取權。如需其他所需許可，請參閱 文件。

AmazonTimestreamInfluxDBServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 3 月 14 日 18：53 UTC
- 編輯時間：2024 年 3 月 14 日 18：53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTimestreamReadOnlyAccess

描述：提供 Amazon Timestream 的唯讀存取權。政策也提供取消任何執行中查詢的許可。如果使用客戶受管 CMK，請參閱 文件以取得所需的其他許可。

AmazonTimestreamReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonTimestreamReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 9 月 30 日，UTC 21：47
- 編輯時間：2024 年 6 月 5 日 19：11 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonTimestreamReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
```

```
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks",
        "timestream:DescribeAccountSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTranscribeFullAccess

描述：提供 Amazon Transcribe 操作的完整存取權

AmazonTranscribeFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonTranscribeFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 4 月 4 日 16：06 UTC

- **編輯時間**：2018 年 4 月 4 日 16：06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonTranscribeReadOnlyAccess

描述：提供 Amazon Transcribe 唯讀操作的存取權

AmazonTranscribeReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonTranscribeReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 4 月 4 日 16：05 UTC
- 編輯時間：2018 年 4 月 4 日 16：05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonVerifiedPermissionsFullAccess

描述：提供已驗證許可的完整存取權

AmazonVerifiedPermissionsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonVerifiedPermissionsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 10 月 11 日 18：19 UTC
- 編輯時間：2024 年 10 月 11 日 18：19 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVerifiedPermissionsFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:CreatePolicyStore",
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:*"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonVerifiedPermissionsReadOnlyAccess

描述：提供 Verified Permissions 服務的唯讀存取權。

`AmazonVerifiedPermissionsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonVerifiedPermissionsReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 10 月 11 日 18：25 UTC
- 編輯時間：2024 年 10 月 11 日 18：25 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVerifiedPermissionsReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
```

```
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyTemplates"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonVPCCrossAccountNetworkInterfaceOperations

描述：提供建立網路介面並將其連接至跨帳戶資源的存取權

AmazonVPCCrossAccountNetworkInterfaceOperations 是 AWS 受管政策。

使用此政策

您可以將 AmazonVPCCrossAccountNetworkInterfaceOperations 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 7 月 18 日 20：47 UTC
- 編輯時間：2023 年 9 月 25 日 15：12 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonVPCFullAccess

描述：透過 提供 Amazon VPC 的完整存取權 AWS 管理主控台。

AmazonVPCFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonVPCFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:AssociateSecurityGroupVpc",
        "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:DescribeSecurityGroupVpcAssociations",
        "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:DisassociateSecurityGroupVpc",
        "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

描述：提供描述 AWS 資源、執行 Network Access Analyzer，以及在 Network Insights Access Scope 和 Network Insights Access Scope Analysis 上建立或刪除標籤的許可。

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 6 月 15 日 22：56 UTC
- 編輯時間：2024 年 5 月 15 日 21：40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScopeAnalysis",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
```

```
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAccessScopeAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-access-scope/*",
        "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
```

```
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonVPCReachabilityAnalyzerFullAccessPolicy

描述：提供描述 AWS 資源、執行 Reachability Analyzer，以及在 Network Insights 路徑和 Network Insights 分析上建立或刪除標籤的許可。

`AmazonVPCReachabilityAnalyzerFullAccessPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonVPCReachabilityAnalyzerFullAccessPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 6 月 14 日 20：12 UTC
- 編輯時間：2024 年 5 月 15 日 20：47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
```

```
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

描述：此政策連接到角色 IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess。當管理帳戶啟用 Reachability Analyzer 的受信任存取時，此角色會部署到組織中的成員帳戶。它提供使用 Reachability Analyzer 主控台從整個組織檢視資源的許可。

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2023 年 5 月 1 日 20：38 UTC
- **編輯時間**：2023 年 5 月 1 日 20：38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonVPCReadOnlyAccess

描述：透過 提供 Amazon VPC 的唯讀存取權 AWS 管理主控台。

AmazonVPCReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonVPCReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:DescribeSecurityGroupVpcAssociations",
        "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonWorkDocsFullAccess

描述：透過 提供 Amazon WorkDocs 的完整存取權 AWS 管理主控台

AmazonWorkDocsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkDocsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 4 月 16 日，UTC 23：05
- 編輯時間：2020 年 4 月 16 日，23：05 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkDocsReadOnlyAccess

描述：透過 提供 Amazon WorkDocs 的唯讀存取權 AWS 管理主控台

`AmazonWorkDocsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonWorkDocsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 1 月 8 日，UTC 23：49
- 編輯時間：2020 年 1 月 8 日 23：49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkMailEventsServiceRolePolicy

描述：允許存取 AWS 服務 Amazon WorkMail Events 使用或管理的資源

`AmazonWorkMailEventsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 4 月 16 日 16：52 UTC

- **編輯時間**：2019 年 4 月 16 日 16：52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkMailFullAccess

描述：提供 WorkMail、 Directory Service、SES、EC2 的完整存取權，以及 KMS 中繼資料的讀取存取權。

`AmazonWorkMailFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkMailFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2020 年 12 月 21 日 14：13 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailFullAccess

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkMailMessageFlowFullAccess

描述：WorkMail 訊息流程 APIs的完整存取權

AmazonWorkMailMessageFlowFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkMailMessageFlowFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2021 年 2 月 11 日 11：08 UTC
- **編輯時間**：2021 年 2 月 11 日 11：08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkMailMessageFlowReadOnlyAccess

描述：唯讀存取 GetRawMessageContent API 的 WorkMail 訊息

AmazonWorkMailMessageFlowReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkMailMessageFlowReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 1 月 28 日 12：40 UTC
- 編輯時間：2021 年 1 月 28 日 12：40 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonWorkMailReadOnlyAccess

描述：提供 WorkMail 和 SES 的唯讀存取權。

AmazonWorkMailReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkMailReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2019 年 7 月 25 日 08：24 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkSpacesAdmin

描述：透過 AWS SDK 和 CLI 提供 Amazon WorkSpaces 管理動作的存取權。

`AmazonWorkSpacesAdmin` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonWorkSpacesAdmin` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 9 月 22 日，UTC 22：21
- 編輯時間：2024 年 6 月 27 日 17：16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonWorkSpacesAdmin",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateWorkspacesPool",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces:DeleteTags",
        "workspaces:DeregisterWorkspaceDirectory",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "workspaces:DescribeWorkspacesPoolSessions",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyStreamingProperties",
        "workspaces:ModifyWorkspaceCreationProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:RegisterWorkspaceDirectory",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
```

```
        "workspaces:StartWorkspacesPool",
        "workspaces:StopWorkspaces",
        "workspaces:StopWorkspacesPool",
        "workspaces:TerminateWorkspaces",
        "workspaces:TerminateWorkspacesPool",
        "workspaces:TerminateWorkspacesPoolSession",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonWorkSpacesApplicationManagerAdminAccess

描述：提供在 Amazon WorkSpaces Application Manager 中封裝應用程式的管理員存取權。

`AmazonWorkSpacesApplicationManagerAdminAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonWorkSpacesApplicationManagerAdminAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 4 月 9 日 14：03 UTC
- 編輯時間：2015 年 4 月 9 日 14：03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkspacesPCAAccess

描述：此受管政策提供 中 AWS Certificate Manager Private CA 資源的完整管理存取權， AWS 帳戶以進行憑證型身分驗證。

AmazonWorkspacesPCAAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkspacesPCAAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 11 月 8 日 00：25 UTC
- 編輯時間：2022 年 11 月 8 日 00：25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkSpacesPoolServiceAccess

描述：此政策提供 AWS WorkSpaces 服務存取啟動工作區集區所需的客戶帳戶資源

AmazonWorkSpacesPoolServiceAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkSpacesPoolServiceAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 6 月 27 日 16：21 UTC
- 編輯時間：2024 年 6 月 27 日 16：21 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProvisioningWorkSpacesPoolPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "WorkSpacesPoolS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::wspool-logs-*",
        "arn:aws:s3:::wspool-app-settings-*",
        "arn:aws:s3:::wspool-home-folder-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkSpacesSecureBrowserReadOnly

描述：透過 、 AWS 管理主控台 SDK 和 CLI 提供 Amazon WorkSpaces 安全瀏覽器及其相依性的唯讀存取權。

AmazonWorkSpacesSecureBrowserReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkSpacesSecureBrowserReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 6 月 24 日 20：01 UTC
- 編輯時間：2024 年 6 月 24 日 20：01 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "WorkSpacesSecureBrowser",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetIpAccessSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListIpAccessSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Sid" : "Dependencies",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkSpacesSelfServiceAccess

描述：提供 Amazon WorkSpaces 後端服務的存取權，以執行工作區自助服務動作

AmazonWorkSpacesSelfServiceAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkSpacesSelfServiceAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 6 月 27 日 19：22 UTC
- 編輯時間：2019 年 6 月 27 日 19：22 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkSpacesServiceAccess

描述：提供客戶對 AWS WorkSpaces 服務的存取權，以啟動工作區。

`AmazonWorkSpacesServiceAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonWorkSpacesServiceAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 6 月 27 日 19：19 UTC
- 編輯時間：2020 年 3 月 18 日 23：32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonWorkSpacesThinClientFullAccess

描述：提供對 Amazon WorkSpaces 精簡型客戶端的完整存取權，以及對所需相關服務的有限存取權

`AmazonWorkSpacesThinClientFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonWorkSpacesThinClientFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 8 月 9 日 07：25 UTC

- **編輯時間**：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientFullAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitoring.thinclient.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy

描述：允許存取 AWS 服務 Amazon WorkSpaces 精簡型客戶端監控使用或管理的資源

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 6 月 13 日 19：37 UTC
- 編輯時間：2025 年 6 月 13 日 19：37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkSpacesThinClientReadOnlyAccess

描述：提供 Amazon WorkSpaces 精簡型客戶端及其相依性的唯讀存取權

AmazonWorkSpacesThinClientReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonWorkSpacesThinClientReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 7 月 19 日 08：50 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientReadOnlyAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:GetDevice",
```

```
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkSpacesWebReadOnly

描述：透過 、 AWS 管理主控台 SDK 和 CLI 提供 Amazon WorkSpaces Web 及其相依性的唯讀存取權。

`AmazonWorkSpacesWebReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AmazonWorkSpacesWebReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 11 月 30 日 14：20 UTC
- 編輯時間：2022 年 11 月 2 日 20：20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmazonWorkSpacesWebServiceRolePolicy

描述：允許存取 Amazon WorkSpaces Web 使用或管理的 AWS 服務 和 資源

AmazonWorkSpacesWebServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 30 日 13：15 UTC
- 編輯時間：2022 年 12 月 15 日 22：46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AmazonZocaloFullAccess

描述：提供 Amazon Zocalo 的完整存取權。

AmazonZocaloFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonZocaloFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC
- ARN: arn:aws:iam::aws:policy/AmazonZocaloFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AmazonZocaloReadOnlyAccess

描述：提供 Amazon Zocalo 的唯讀存取權

AmazonZocaloReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AmazonZocaloReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AmplifyBackendDeployFullAccess

描述：提供 Amplify 完整存取許可，以透過 AWS 雲端 開發套件 (AWS CDK) 部署 Amplify 後端資源 (AWS AppSync、Amazon Cognito、Amazon S3 和其他相關服務）

AmplifyBackendDeployFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AmplifyBackendDeployFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 10 月 6 日 21：32 UTC
- 編輯時間：2024 年 11 月 14 日 19：09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableFunctionResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
```

```
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingListTags",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListTags"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ]
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/amplify-*:*",
        "arn:aws:logs:*:*:log-group:amplify-*:*"
      ]
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*",
        "arn:aws:ssm:*:*:parameter/cdk-bootstrap/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:DeleteParameters"
```

```
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyDiscoverRDSVpcConfig",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBProxies",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "ec2:DescribeSubnets",
        "rds:DescribeDBSubnetGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db-proxy:*",
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

APIGatewayServiceRolePolicy

描述：允許 API Gateway 代表客戶管理相關聯的 AWS 資源。

APIGatewayServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 20 日 17：23 UTC
- 編輯時間：2021 年 7 月 12 日 22：24 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AppIntegrationsServiceLinkedRolePolicy

描述：允許 AppIntegrations 代表您管理 AppFlow 資源和發佈 CloudWatch 指標資料。

AppIntegrationsServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 9 月 30 日 19：42 UTC
- 編輯時間：2022 年 9 月 30 日 19：42 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ApplicationAutoScalingForAmazonAppStreamAccess

描述：為 Amazon AppStream 啟用 Application Autoscaling 的政策

`ApplicationAutoScalingForAmazonAppStreamAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ApplicationAutoScalingForAmazonAppStreamAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 2 月 6 日 21：39 UTC
- 編輯時間：2017 年 2 月 6 日 21：39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

描述：啟用對 Application Discovery Service Continuous Export 功能使用或管理 AWS 服務 的資源的存取

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 8 月 9 日 20：22 UTC
- 編輯時間：2018 年 8 月 13 日，UTC 22：31
- ARN: arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AppRunnerNetworkingServiceRolePolicy

描述：Alcan AWS AppRunner Networking 可代表您管理相關 AWS 資源。

AppRunnerNetworkingServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 1 月 12 日 21：02 UTC

- **編輯時間**：2022 年 1 月 12 日 21：02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AppRunnerServiceRolePolicy

描述：Alcan AWS AppRunner 代表您管理相關 AWS 資源。

AppRunnerServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- **建立時間**：2021 年 5 月 14 日，UTC 19：15
- **編輯時間**：2021 年 5 月 14 日 19：15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AppStudioServiceRolePolicy

描述：允許 AppStudio 代表您管理相關聯的 AWS 資源。

AppStudioServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 7 月 10 日 05：01 UTC
- 編輯時間：2025 年 3 月 13 日 20：37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AppStudioServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppStudioResourcePermissionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appstudio/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "IsAppStudioSecret"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/IsAppStudioSecret" : "true"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appstudio"
        }
      }
    },
    {
      "Sid" : "AppStudioResourceWritePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AuroraDsqlServiceLinkedRolePolicy

描述：Amazon Aurora DSQL 服務連結角色的政策

`AuroraDsqlServiceLinkedRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 12 月 3 日 15：06 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AuroraDsqlServiceLinkedRolePolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AuroraDSQL",
            "AWS/Usage"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AutoScalingConsoleFullAccess

描述：透過 提供 Auto Scaling 的完整存取權 AWS 管理主控台。

`AutoScalingConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AutoScalingConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 1 月 12 日 19：43 UTC
- 編輯時間：2018 年 2 月 6 日 23：15 UTC
- ARN: arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AutoScalingConsoleReadOnlyAccess

描述：透過 提供 Auto Scaling 的唯讀存取權 AWS 管理主控台。

`AutoScalingConsoleReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AutoScalingConsoleReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 1 月 12 日 19：48 UTC
- 編輯時間：2017 年 1 月 12 日 19：48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AutoScalingFullAccess

描述：提供 Auto Scaling 的完整存取權。

`AutoScalingFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AutoScalingFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 1 月 12 日 19：31 UTC
- 編輯時間：2018 年 2 月 6 日 21：59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AutoScalingNotificationAccessRole

描述：AutoScaling Notification Access 服務角色的預設政策。

`AutoScalingNotificationAccessRole` 是 AWS 受管政策。

使用此政策

您可以將 `AutoScalingNotificationAccessRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AutoScalingReadOnlyAccess

描述：提供 Auto Scaling 的唯讀存取權。

`AutoScalingReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AutoScalingReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 1 月 12 日 19：39 UTC
- 編輯時間：2017 年 1 月 12 日 19：39 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AutoScalingServiceRolePolicy

描述：允許存取 AWS 服務 和 Auto Scaling 使用或管理的資源

`AutoScalingServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 1 月 8 日 23：10 UTC
- 編輯時間：2025 年 11 月 12 日 18：19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateReplaceRootVolumeTask",
        "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"
      ],
      "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" : "*"
    },
    {
      "Sid" : "ResourceGroupsManagement",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWS-SSM-Automation-DiagnosisBucketPolicy

描述：提供存取 SSM 診斷 S3 儲存貯體的許可，以診斷和修復問題。

AWS-SSM-Automation-DiagnosisBucketPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWS-SSM-Automation-DiagnosisBucketPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 15 日 23：31 UTC
- 編輯時間：2024 年 11 月 15 日 23：31 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

描述：透過執行自動化文件中定義的活動，提供診斷 SSM 服務問題的許可，主要用於透過觸發成員帳戶中的子自動化，在跨帳戶跨區域設定中執行自動化文件。

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2024 年 11 月 16 日 00：01 UTC
- **編輯時間**：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

描述：透過執行自動化文件中定義的活動，提供診斷 SSM 服務問題的許可，主要用於透過診斷所有節點的 SSM 服務運作狀態，在目標帳戶/區域中設定中執行自動化文件。

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 16 日 00：08 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkAcls"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationStepExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeActivations",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
```

```
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

描述：透過提供 SSM 自動化所需的組織特定許可，為營運帳戶提供診斷未受管節點的許可，以提取組織根目錄中的成員帳戶清單，透過允許在目標帳戶/區域中擔任執行角色來觸發跨帳戶跨區域執行。

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 16 日 00：11 UTC
- 編輯時間：2024 年 11 月 16 日 00：11 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinOrg",
```

```
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWS-SSM-RemediationAutomation-AdministrationRolePolicy

描述：透過執行自動化文件中定義的活動，提供修復 SSM 服務問題的許可，主要用於透過觸發成員帳戶中的子自動化，在跨帳戶跨區域設定中執行自動化文件。

AWS-SSM-RemediationAutomation-AdministrationRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWS-SSM-RemediationAutomation-AdministrationRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 16 日 00：14 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-AdministrationRolePolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
```

```
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWS-SSM-RemediationAutomation-ExecutionRolePolicy

描述：透過執行自動化文件中定義的活動，提供修復 SSM 服務問題的許可，主要用於透過修復所有節點的 SSM 服務運作狀態，在目標帳戶/區域設定中執行自動化文件。

AWS-SSM-RemediationAutomation-ExecutionRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWS-SSM-RemediationAutomation-ExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 16 日 00：17 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-ExecutionRolePolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateVpcEndpointForTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "RestrictCreateVpcEndpointForSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.ssm",
            "com.amazonaws.*.ssmmessages",
            "com.amazonaws.*.ec2messages"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint"
        }
      }
    },
    {
      "Sid" : "RestrictCreateVpcEndpointWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint",
          "ec2:CreateAction" : [
            "CreateVpcEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "AllowModifyVpcAttributeForDns",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Attribute" : [
            "EnableDnsSupport",
            "EnableDnsHostnames"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateForTaggedResource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateTagRule",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess",
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupEgress",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateSecurityGroupForVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "AllowCreateSecurityGroupWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowTagCreationForSecurityGroupTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

描述：提供 SSM 自動化所需的組織特定許可，藉此為操作帳戶提供修復未受管節點的許可，以提取組織根目錄中的成員帳戶清單，透過允許在目標帳戶/區域中擔任執行角色來觸發跨帳戶跨區域執行。

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 11 月 16 日 00：25 UTC
- 編輯時間：2024 年 11 月 16 日 00：25 UTC
- ARN: arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWS_ConfigRole

描述：Config AWS 服務角色的預設政策。提供 Config AWS 追蹤 AWS 資源變更所需的許可。

AWS_ConfigRole 是 AWS 受管政策。

使用此政策

您可以將 AWS_ConfigRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 9 月 15 日，20：30 UTC

- **編輯時間**：2026 年 2 月 24 日 22：42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

政策版本

政策版本： v67 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID1",
      "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:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
```

```
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
```

```
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListTagsForResource",
        "applicationinsights:DescribeApplication",
        "applicationinsights:DescribeComponent",
        "applicationinsights:DescribeLogPattern",
        "applicationinsights:ListApplications",
        "applicationinsights:ListComponents",
        "applicationinsights:ListLogPatterns",
        "applicationinsights:ListLogPatternSets",
        "applicationinsights:ListTagsForResource",
        "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:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
```

```
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApi",
        "appsync:GetApiAssociation",
        "appsync:GetApiCache",
        "appsync:GetChannelNamespace",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListApis",
        "appsync:ListChannelNamespaces",
        "appsync:ListDataSources",
        "appsync:ListDomainNames",
        "appsync:ListGraphqlApis",
        "appsync:ListSourceApiAssociations",
        "appsync:ListTagsForResource",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:DescribeWorkspace",
        "aps:DescribeWorkspaceConfiguration",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
```

```
            "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",
            "b2bi:GetCapability",
            "b2bi:GetPartnership",
            "b2bi:GetProfile",
            "b2bi:GetTransformer",
            "b2bi:ListCapabilities",
            "b2bi:ListPartnerships",
            "b2bi:ListProfiles",
            "b2bi:ListTagsForResource",
            "b2bi:ListTransformers",
            "backup-gateway:GetHypervisor",
            "backup-gateway:ListHypervisors",
            "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:GetRestoreTestingPlan",
            "backup:GetRestoreTestingSelection",
```

```
            "backup:ListBackupPlans",
            "backup:ListBackupSelections",
            "backup:ListBackupVaults",
            "backup:ListFrameworks",
            "backup:ListRecoveryPointsByBackupVault",
            "backup:ListReportPlans",
            "backup:ListRestoreTestingPlans",
            "backup:ListRestoreTestingSelections",
            "backup:ListTags",
            "batch:DescribeComputeEnvironments",
            "batch:DescribeConsumableResource",
            "batch:DescribeJobDefinitions",
            "batch:DescribeJobQueues",
            "batch:DescribeSchedulingPolicies",
            "batch:DescribeServiceEnvironments",
            "batch:ListConsumableResources",
            "batch:ListSchedulingPolicies",
            "batch:ListTagsForResource",
            "bcm-data-exports:GetExport",
            "bcm-data-exports:ListExports",
            "bcm-data-exports:ListTagsForResource",
            "bedrock-agentcore:GetAgentRuntime",
            "bedrock-agentcore:GetAgentRuntimeEndpoint",
            "bedrock-agentcore:GetBrowser",
            "bedrock-agentcore:GetCodeInterpreter",
            "bedrock-agentcore:GetGateway",
            "bedrock-agentcore:GetGatewayTarget",
            "bedrock-agentcore:GetMemory",
            "bedrock-agentcore:GetWorkloadIdentity",
            "bedrock-agentcore:ListAgentRuntimeEndpoints",
            "bedrock-agentcore:ListAgentRuntimes",
            "bedrock-agentcore:ListBrowsers",
            "bedrock-agentcore:ListCodeInterpreters",
            "bedrock-agentcore:ListGateways",
            "bedrock-agentcore:ListGatewayTargets",
            "bedrock-agentcore:ListMemories",
            "bedrock-agentcore:ListTagsForResource",
            "bedrock-agentcore:ListWorkloadIdentities",
            "bedrock:GetAgent",
            "bedrock:GetAgentActionGroup",
            "bedrock:GetAgentAlias",
            "bedrock:GetAgentCollaborator",
            "bedrock:GetAgentKnowledgeBase",
            "bedrock:GetDataAutomationProject",
```

```
            "bedrock:GetDataSource",
            "bedrock:GetFlow",
            "bedrock:GetFlowAlias",
            "bedrock:GetFlowVersion",
            "bedrock:GetGuardrail",
            "bedrock:GetInferenceProfile",
            "bedrock:GetKnowledgeBase",
            "bedrock:GetModelInvocationLoggingConfiguration",
            "bedrock:ListAgentActionGroups",
            "bedrock:ListAgentAliases",
            "bedrock:ListAgentCollaborators",
            "bedrock:ListAgentKnowledgeBases",
            "bedrock:ListAgents",
            "bedrock:ListDataAutomationProjects",
            "bedrock:ListDataSources",
            "bedrock:ListFlowAliases",
            "bedrock:ListFlows",
            "bedrock:ListFlowVersions",
            "bedrock:ListGuardrails",
            "bedrock:ListInferenceProfiles",
            "bedrock:ListKnowledgeBases",
            "bedrock:ListPromptRouters",
            "bedrock:ListPrompts",
            "bedrock:ListTagsForResource",
            "billing:GetBillingView",
            "billing:ListBillingViews",
            "billing:ListSourceViewsForBillingView",
            "billing: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:DescribeCostCategoryDefinition",
            "ce:GetAnomalyMonitors",
            "ce:GetAnomalySubscriptions",
            "ce:ListCostCategoryDefinitions",
```

```
        "ce:ListTagsForResource",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetAnycastIpList",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
```

```
            "cloudfront:GetConnectionGroup",
            "cloudfront:GetContinuousDeploymentPolicy",
            "cloudfront:GetDistributionTenant",
            "cloudfront:GetFunction",
            "cloudfront:GetKeyGroup",
            "cloudfront:GetMonitoringSubscription",
            "cloudfront:GetOriginAccessControl",
            "cloudfront:GetOriginRequestPolicy",
            "cloudfront:GetPublicKey",
            "cloudfront:GetRealtimeLogConfig",
            "cloudfront:GetResponseHeadersPolicy",
            "cloudfront:GetVpcOrigin",
            "cloudfront:ListAnycastIpLists",
            "cloudfront:ListCachePolicies",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "cloudfront:ListConnectionGroups",
            "cloudfront:ListContinuousDeploymentPolicies",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionTenants",
            "cloudfront:ListFunctions",
            "cloudfront:ListKeyGroups",
            "cloudfront:ListKeyValueStores",
            "cloudfront:ListOriginAccessControls",
            "cloudfront:ListOriginRequestPolicies",
            "cloudfront:ListPublicKeys",
            "cloudfront:ListRealtimeLogConfigs",
            "cloudfront:ListResponseHeadersPolicies",
            "cloudfront:ListTagsForResource",
            "cloudfront:ListVpcOrigins",
            "cloudtrail:DescribeTrails",
            "cloudTrail:GetChannel",
            "cloudtrail:GetDashboard",
            "cloudtrail:GetEventConfiguration",
            "cloudtrail:GetEventDataStore",
            "cloudtrail:GetEventSelectors",
            "cloudtrail:GetInsightSelectors",
            "cloudtrail:GetResourcePolicy",
            "cloudtrail:GetTrailStatus",
            "cloudTrail:ListChannels",
            "cloudtrail:ListDashboards",
            "cloudtrail:ListEventDataStores",
            "cloudtrail:ListTags",
            "cloudtrail:ListTrails",
            "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetFleets",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListFleets",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections: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:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
```

```
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
```

```
            "connect:DescribeInstance",
            "connect:DescribeInstanceStorageConfig",
            "connect:DescribePhoneNumber",
            "connect:DescribePredefinedAttribute",
            "connect:DescribePrompt",
            "connect:DescribeQueue",
            "connect:DescribeQuickConnect",
            "connect:DescribeRoutingProfile",
            "connect:DescribeRule",
            "connect:DescribeSecurityProfile",
            "connect:DescribeTrafficDistributionGroup",
            "connect:DescribeUser",
            "connect:DescribeUserHierarchyGroup",
            "connect:DescribeView",
            "connect:GetTaskTemplate",
            "connect:ListAgentStatuses",
            "connect:ListApprovedOrigins",
            "connect:ListEvaluationForms",
            "connect:ListEvaluationFormVersions",
            "connect:ListHoursOfOperationOverrides",
            "connect:ListHoursOfOperations",
            "connect:ListInstanceAttributes",
            "connect:ListInstances",
            "connect:ListInstanceStorageConfigs",
            "connect:ListIntegrationAssociations",
            "connect:ListPhoneNumbers",
            "connect:ListPhoneNumbersV2",
            "connect:ListPredefinedAttributes",
            "connect:ListPrompts",
            "connect:ListQueueQuickConnects",
            "connect:ListQueues",
            "connect:ListQuickConnects",
            "connect:ListRoutingProfileManualAssignmentQueues",
            "connect:ListRoutingProfileQueues",
            "connect:ListRoutingProfiles",
            "connect:ListRules",
            "connect:ListSecurityKeys",
            "connect:ListSecurityProfileApplications",
            "connect:ListSecurityProfilePermissions",
            "connect:ListSecurityProfiles",
            "connect:ListTagsForResource",
            "connect:ListTaskTemplates",
            "connect:ListTrafficDistributionGroups",
            "connect:ListUserHierarchyGroups",
```

```
            "connect:ListUsers",
            "connect:ListViews",
            "connect:ListViewVersions",
            "connect:SearchAvailablePhoneNumbers",
            "controltower:GetLandingZone",
            "controltower:ListLandingZones",
            "cur:DescribeReportDefinitions",
            "cur:ListTagsForResource",
            "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",
            "databrew:ListTagsForResource",
            "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",
            "datazone:GetDomain",
            "datazone:GetDomainUnit",
            "datazone:GetEnvironmentAction",
            "datazone:GetEnvironmentBlueprintConfiguration",
            "datazone:GetEnvironmentProfile",
            "datazone:GetGroupProfile",
            "datazone:GetSubscriptionTarget",
            "datazone:GetUserProfile",
```

```
            "datazone:ListDomains",
            "datazone:ListDomainUnitsForParent",
            "datazone:ListEntityOwners",
            "datazone:ListEnvironmentActions",
            "datazone:ListEnvironmentBlueprintConfigurations",
            "datazone:ListEnvironmentProfiles",
            "datazone:ListPolicyGrants",
            "datazone:ListProjectMemberships",
            "datazone:ListSubscriptionTargets",
            "datazone:SearchGroupProfiles",
            "datazone:SearchUserProfiles",
            "dax:DescribeClusters",
            "dax:DescribeParameterGroups",
            "dax:DescribeParameters",
            "dax:DescribeSubnetGroups",
            "dax:ListTags",
            "deadline:GetFarm",
            "deadline:GetFleet",
            "deadline:GetLicenseEndpoint",
            "deadline:GetMonitor",
            "deadline:GetQueue",
            "deadline:GetQueueEnvironment",
            "deadline:GetQueueFleetAssociation",
            "deadline:GetQueueLimitAssociation",
            "deadline:GetStorageProfile",
            "deadline:ListFarms",
            "deadline:ListFleets",
            "deadline:ListLicenseEndpoints",
            "deadline:ListMonitors",
            "deadline:ListQueueEnvironments",
            "deadline:ListQueueFleetAssociations",
            "deadline:ListQueueLimitAssociations",
            "deadline:ListQueues",
            "deadline:ListStorageProfiles",
            "deadline:ListTagsForResource",
            "detective:ListGraphs",
            "detective:ListOrganizationAdminAccount",
            "detective:ListTagsForResource",
            "devicefarm:GetInstanceProfile",
            "devicefarm:GetNetworkProfile",
            "devicefarm:GetProject",
            "devicefarm:GetTestGridProject",
            "devicefarm:ListInstanceProfiles",
            "devicefarm:ListNetworkProfiles",
```

```
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListDataProviders",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
```

```
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetRouteServerAssociations",
        "ec2:GetRouteServerPropagations",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "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:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
```

```
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeListenerAttributes",
        "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:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "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:GetTargetAccountConfiguration",
            "fis:ListExperimentTemplates",
            "fis:ListTagsForResource",
            "fis:ListTargetAccountConfigurations",
            "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:GetListElements",
            "frauddetector:GetListsMetadata",
```

```
        "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:DescribeContainerFleet",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
```

```
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "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:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
```

```
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:GetDeployment",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "greengrass:ListDeployments",
        "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:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
```

```
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "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:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
```

```
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
```

```
            "iot:DescribeDomainConfiguration",
            "iot:DescribeFleetMetric",
            "iot:DescribeJob",
            "iot:DescribeJobTemplate",
            "iot:DescribeMitigationAction",
            "iot:DescribeProvisioningTemplate",
            "iot:DescribeRoleAlias",
            "iot:DescribeScheduledAudit",
            "iot:DescribeSecurityProfile",
            "iot:DescribeThing",
            "iot:DescribeThingGroup",
            "iot:DescribeThingType",
            "iot:GetCommand",
            "iot:GetPackage",
            "iot:GetPackageVersion",
            "iot:GetPolicy",
            "iot:GetTopicRule",
            "iot:GetTopicRuleDestination",
            "iot:GetV2LoggingOptions",
            "iot:ListAuthorizers",
            "iot:ListBillingGroups",
            "iot:ListCACertificates",
            "iot:ListCertificateProviders",
            "iot:ListCertificates",
            "iot:ListCommands",
            "iot:ListCustomMetrics",
            "iot:ListDimensions",
            "iot:ListDomainConfigurations",
            "iot:ListFleetMetrics",
            "iot:ListJobTemplates",
            "iot:ListMitigationActions",
            "iot:ListPackages",
            "iot:ListPackageVersions",
            "iot:ListPolicies",
            "iot:ListProvisioningTemplates",
            "iot:ListRoleAliases",
            "iot:ListScheduledAudits",
            "iot:ListSecurityProfiles",
            "iot:ListSecurityProfilesForTarget",
            "iot:ListTagsForResource",
            "iot:ListTargetsForSecurityProfile",
            "iot:ListThingGroups",
            "iot:ListThingTypes",
            "iot:ListTopicRuleDestinations",
```

```
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigRoleStatementID2",
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
```

```
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "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:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
```

```
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat: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:DescribeCustomPlugin",
            "kafkaconnect:DescribeWorkerConfiguration",
            "kafkaconnect:ListConnectors",
            "kafkaconnect:ListCustomPlugins",
            "kafkaconnect:ListTagsForResource",
            "kafkaconnect:ListWorkerConfigurations",
            "kendra-ranking:DescribeRescoreExecutionPlan",
            "kendra-ranking:ListRescoreExecutionPlans",
            "kendra-ranking:ListTagsForResource",
            "kendra:DescribeIndex",
            "kendra:ListDataSources",
            "kendra:ListIndices",
            "kendra:ListTagsForResource",
            "kinesis:DescribeStreamConsumer",
            "kinesis:DescribeStreamSummary",
            "kinesis:GetResourcePolicy",
            "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:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "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:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
```

```
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "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:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
```

```
        "mediaconnect:DescribeGateway",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
```

```
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "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",
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "mq:ListTags",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
```

```
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "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:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:GetResourcePolicy",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
```

```
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
```

```
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "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:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
```

```
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "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:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
```

```
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "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",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "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",
            "route53profiles:GetProfile",
            "route53profiles:GetProfileAssociation",
            "route53profiles:ListProfileAssociations",
            "route53profiles:ListProfiles",
            "route53profiles:ListTagsForResource",
            "route53resolver:GetFirewallDomainList",
            "route53resolver:GetFirewallRuleGroup",
            "route53resolver:GetFirewallRuleGroupAssociation",
            "route53resolver:GetOutpostResolver",
            "route53resolver:GetResolverDnssecConfig",
            "route53resolver:GetResolverEndpoint",
            "route53resolver:GetResolverQueryLogConfig",
            "route53resolver:GetResolverQueryLogConfigAssociation",
            "route53resolver:GetResolverRule",
            "route53resolver:GetResolverRuleAssociation",
            "route53resolver:ListFirewallDomainLists",
            "route53resolver:ListFirewallDomains",
            "route53resolver:ListFirewallRuleGroupAssociations",
            "route53resolver:ListFirewallRuleGroups",
            "route53resolver:ListFirewallRules",
            "route53resolver:ListOutpostResolvers",
            "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:GetAccessGrant",
            "s3:GetAccessGrantsInstance",
            "s3:GetAccessGrantsLocation",
            "s3:GetAccessPoint",
            "s3:GetAccessPointForObjectLambda",
            "s3:GetAccessPointPolicy",
            "s3:GetAccessPointPolicyForObjectLambda",
            "s3:GetAccessPointPolicyStatus",
            "s3:GetAccessPointPolicyStatusForObjectLambda",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucketAbac",
            "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:GetStorageLensGroup",
            "s3:ListAccessGrants",
            "s3:ListAccessGrantsInstances",
            "s3:ListAccessGrantsLocations",
            "s3:ListAccessPoints",
            "s3:ListAccessPointsForObjectLambda",
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "s3:ListMultiRegionAccessPoints",
            "s3:ListStorageLensConfigurations",
            "s3:ListStorageLensGroups",
            "s3:ListTagsForResource",
            "s3express:GetBucketPolicy",
            "s3express:GetEncryptionConfiguration",
            "s3express:GetLifecycleConfiguration",
            "s3express:ListAllMyDirectoryBuckets",
            "s3tables:GetTableBucket",
            "s3tables:GetTableBucketEncryption",
            "s3tables:GetTableBucketMaintenanceConfiguration",
            "s3tables:GetTableBucketMetricsConfiguration",
            "s3tables:GetTableBucketPolicy",
            "s3tables:GetTableBucketStorageClass",
            "s3tables:ListTableBuckets",
            "s3tables:ListTagsForResource",
            "s3vectors:GetVectorBucketPolicy",
            "s3vectors:ListVectorBuckets",
            "sagemaker:DescribeApp",
            "sagemaker:DescribeAppImageConfig",
            "sagemaker:DescribeCluster",
            "sagemaker:DescribeCodeRepository",
            "sagemaker:DescribeDataQualityJobDefinition",
            "sagemaker:DescribeDeviceFleet",
            "sagemaker:DescribeDomain",
            "sagemaker:DescribeEndpoint",
            "sagemaker:DescribeEndpointConfig",
            "sagemaker:DescribeFeatureGroup",
            "sagemaker:DescribeImage",
            "sagemaker:DescribeImageVersion",
            "sagemaker:DescribeInferenceComponent",
            "sagemaker:DescribeInferenceExperiment",
            "sagemaker:DescribeMlflowTrackingServer",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeModelBiasJobDefinition",
            "sagemaker:DescribeModelCard",
```

```
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
```

```
            "sagemaker:ListSpaces",
            "sagemaker:ListStudioLifecycleConfigs",
            "sagemaker:ListTags",
            "sagemaker:ListUserProfiles",
            "sagemaker:ListWorkteams",
            "scheduler:GetSchedule",
            "scheduler:GetScheduleGroup",
            "scheduler:ListScheduleGroups",
            "scheduler:ListSchedules",
            "scheduler:ListTagsForResource",
            "schemas:DescribeDiscoverer",
            "schemas:DescribeRegistry",
            "schemas:DescribeSchema",
            "schemas:GetResourcePolicy",
            "schemas:ListDiscoverers",
            "schemas:ListRegistries",
            "schemas:ListSchemas",
            "sdb:GetAttributes",
            "sdb:ListDomains",
            "secretsmanager:DescribeSecret",
            "secretsmanager:GetResourcePolicy",
            "secretsmanager:ListSecrets",
            "secretsmanager:ListSecretVersionIds",
            "securityhub:DescribeHub",
            "securityhub:DescribeOrganizationConfiguration",
            "securityhub:DescribeStandardsControls",
            "securityhub:GetAggregatorV2",
            "securityhub:GetAutomationRuleV2",
            "securityhub:GetConfigurationPolicy",
            "securityhub:GetConfigurationPolicyAssociation",
            "securityhub:GetEnabledStandards",
            "securityhub:GetFindingAggregator",
            "securityhub:ListAggregatorsV2",
            "securityhub:ListAutomationRulesV2",
            "securityhub:ListConfigurationPolicies",
            "securityhub:ListConfigurationPolicyAssociations",
            "securityhub:ListEnabledProductsForImport",
            "securityhub:ListFindingAggregators",
            "securityhub:ListTagsForResource",
            "securitylake:GetSubscriber",
            "securitylake:ListDataLakeExceptions",
            "securitylake:ListDataLakes",
            "securitylake:ListLogSources",
            "securitylake:ListSubscribers",
```

```
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetAddonInstance",
        "ses:GetAddonSubscription",
        "ses:GetArchive",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetIngressPoint",
        "ses:GetRelay",
        "ses:GetRuleSet",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListAddonInstances",
        "ses:ListAddonSubscriptions",
        "ses:ListArchives",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListIngressPoints",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListRelays",
```

```
        "ses:ListRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListTagsForResource",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
```

```
            "ssm-incidents:ListTagsForResource",
            "ssm-quicksetup:GetConfigurationManager",
            "ssm-quicksetup:ListConfigurationManagers",
            "ssm-sap:ListTagsForResource",
            "ssm:DescribeAssociation",
            "ssm:DescribeAutomationExecutions",
            "ssm:DescribeDocument",
            "ssm:DescribeDocumentPermission",
            "ssm:DescribeInstanceInformation",
            "ssm:DescribeMaintenanceWindows",
            "ssm:DescribeParameters",
            "ssm:DescribePatchBaselines",
            "ssm:GetAutomationExecution",
            "ssm:GetDefaultPatchBaseline",
            "ssm:GetDocument",
            "ssm:GetPatchBaseline",
            "ssm:GetResourcePolicies",
            "ssm:GetServiceSetting",
            "ssm:ListAssociations",
            "ssm:ListDocuments",
            "ssm:ListResourceDataSync",
            "ssm:ListTagsForResource",
            "sso:DescribeInstanceAccessControlAttributeConfiguration",
            "sso:DescribePermissionSet",
            "sso:GetInlinePolicyForPermissionSet",
            "sso:ListManagedPoliciesInPermissionSet",
            "sso:ListPermissionSets",
            "sso:ListTagsForResource",
            "states:DescribeActivity",
            "states:DescribeStateMachine",
            "states:DescribeStateMachineAlias",
            "states:ListActivities",
            "states:ListStateMachineAliases",
            "states:ListStateMachines",
            "states:ListStateMachineVersions",
            "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",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
```

```
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
```

```
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "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/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAccountActivityAccess

描述：允許使用者存取帳戶活動頁面。

AWSAccountActivityAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAccountActivityAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2026 年 2 月 20 日 20：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountActivityAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAccountManagementFullAccess

描述：提供 AWS 帳戶管理的完整存取權。

`AWSAccountManagementFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSAccountManagementFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 9 月 30 日 23：20 UTC
- 編輯時間：2021 年 9 月 30 日 23：20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSAccountManagementReadOnlyAccess

描述：提供 AWS 帳戶管理的唯讀存取權

`AWSAccountManagementReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSAccountManagementReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 9 月 30 日，UTC 23：29
- 編輯時間：2021 年 9 月 30 日 23：29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAccountSettingsManagementRole

描述：提供管理 AWS 應用程式帳戶所需的許可。

AWSAccountSettingsManagementRole 是 AWS 受管政策。

使用此政策

您可以將 AWSAccountSettingsManagementRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 12 月 11 日 17：49 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountSettingsManagementRole`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:GetAccountInformation",
        "account:CloseAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "payments:ListTagsForResource",
        "payments:UntagResource",
        "payments:TagResource",
        "payments:ListPaymentPreferences",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:MakePayment",
        "payments:UpdatePaymentPreferences",
        "payments:CreatePaymentInstrument",
```

```
        "payments:UpdatePaymentInstrument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetSellerOfRecord"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tax:GetTaxRegistration",
        "tax:PutTaxRegistration",
```

```
        "tax:ListTaxRegistrations",
        "tax:DeleteTaxRegistration",
        "tax:BatchPutTaxRegistration",
        "tax:GetTaxRegistrationDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:ListApplications",
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAccountUsageReportAccess

描述：允許使用者存取帳戶用量報告頁面。

AWSAccountUsageReportAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAccountUsageReportAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC
- ARN: arn:aws:iam::aws:policy/AWSAccountUsageReportAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAgentlessDiscoveryService

描述：提供 Discovery Agentless Connector 向 AWS Application Discovery Service 註冊的存取權。

AWSAgentlessDiscoveryService 是 AWS 受管政策。

使用此政策

您可以將 AWSAgentlessDiscoveryService 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 8 月 2 日 01：35 UTC
- 編輯時間：2020 年 2 月 24 日，23：08 UTC
- ARN: arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppFabricFullAccess

描述：提供對 AWS AppFabric 服務的完整存取權，以及對 S3、Kinesis、KMS 等相依服務的唯讀存取權。

AWSAppFabricFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAppFabricFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 6 月 27 日 19：51 UTC
- 編輯時間：2023 年 6 月 27 日 19：51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSAppFabricReadOnlyAccess

描述：提供對 the AWS AppFabric 的唯讀存取權

AWSAppFabricReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAppFabricReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 6 月 27 日 19：52 UTC
- 編輯時間：2023 年 6 月 27 日 19：52 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSAppFabricServiceRolePolicy

描述：代表您提供 AWS 資源的 AppFabric 存取權

AWSAppFabricServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 6 月 26 日 21：07 UTC
- 編輯時間：2023 年 6 月 26 日 21：07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingAppStreamFleetPolicy

描述：將許可授予 Application Auto Scaling 以存取 AppStream 和 CloudWatch 的政策。

`AWSApplicationAutoscalingAppStreamFleetPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 20 日 19：04 UTC
- 編輯時間：2017 年 10 月 20 日 19：04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSApplicationAutoscalingCassandraTablePolicy

描述：將許可授予 Application Auto Scaling 以存取 Cassandra 和 CloudWatch 的政策。

AWSApplicationAutoscalingCassandraTablePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 3 月 18 日，22：49 UTC
- 編輯時間：2020 年 3 月 18 日 22：49 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSApplicationAutoscalingComprehendEndpointPolicy

描述：將許可授予 Application Auto Scaling 以存取 Comprehend 和 CloudWatch 的政策。

AWSApplicationAutoscalingComprehendEndpointPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 14 日 18：39 UTC
- 編輯時間：2019 年 11 月 14 日 18：39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
```

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoScalingCustomResourcePolicy

描述：將許可授予 Application Auto Scaling 以存取 APIGateway 和 CloudWatch 以進行自訂資源擴展的政策

AWSApplicationAutoScalingCustomResourcePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 6 月 4 日 23：22 UTC
- 編輯時間：2018 年 6 月 4 日 23：22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingDynamoDBTablePolicy

描述：將許可授予 Application Auto Scaling 以存取 DynamoDB 和 CloudWatch 的政策。

AWSApplicationAutoscalingDynamoDBTablePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 20 日，UTC 21：34

- **編輯時間**：2017 年 10 月 20 日，UTC 21：34
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

描述：將許可授予 Application Auto Scaling 以存取 EC2 Spot Fleet 和 CloudWatch 的政策。

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 25 日 18：23 UTC
- 編輯時間：2017 年 10 月 25 日 18：23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingECSServicePolicy

描述：將許可授予 Application Auto Scaling 以存取 EC2 Container Service 和 CloudWatch 的政策。

`AWSApplicationAutoscalingECSServicePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 25 日，UTC 23：53
- 編輯時間：2024 年 10 月 24 日，UTC 20：05
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingElastiCacheRGPolicy

描述：將許可授予 Application Auto Scaling 以存取 Amazon ElastiCache 和 Amazon CloudWatch 的政策。

`AWSApplicationAutoscalingElastiCacheRGPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 8 月 17 日，UTC 23：41

- **編輯時間**：2025 年 3 月 26 日 17：37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheActionsOnAllClusters",
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyCacheCluster",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
```

```
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingEMRInstanceGroupPolicy

描述：將許可授予 Application Auto Scaling 以存取 Elastic Map Reduce 和 CloudWatch 的政策。

AWSApplicationAutoscalingEMRInstanceGroupPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 26 日 00：57 UTC
- 編輯時間：2017 年 10 月 26 日 00：57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingKafkaClusterPolicy

描述：將許可授予 Application Auto Scaling 以存取 Managed Streaming for Apache Kafka 和 CloudWatch 的政策。

`AWSApplicationAutoscalingKafkaClusterPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 8 月 24 日 18：36 UTC
- 編輯時間：2020 年 8 月 24 日 18：36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingLambdaConcurrencyPolicy

描述：將許可授予 Application Auto Scaling 以存取 Lambda 和 CloudWatch 的政策。

`AWSApplicationAutoscalingLambdaConcurrencyPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 10 月 21 日，UTC 20：04
- 編輯時間：2019 年 10 月 21 日，UTC 20：04
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingNeptuneClusterPolicy

描述：將許可授予 Application Auto Scaling 以存取 Amazon Neptune 和 Amazon CloudWatch 的政策。

`AWSApplicationAutoscalingNeptuneClusterPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 9 月 2 日 21：14 UTC
- 編輯時間：2021 年 9 月 2 日 21：14 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingRDSClusterPolicy

描述：將許可授予 Application Auto Scaling 以存取 RDS 和 CloudWatch 的政策。

AWSApplicationAutoscalingRDSClusterPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 17 日 17：46 UTC
- 編輯時間：2018 年 8 月 7 日 19：14 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingSageMakerEndpointPolicy

描述：將許可授予 Application Auto Scaling 以存取 SageMaker 和 CloudWatch 的政策。

AWSApplicationAutoscalingSageMakerEndpointPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 2 月 6 日 19：58 UTC
- 編輯時間：2023 年 11 月 13 日 18：52 UTC

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

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationAutoscalingWorkSpacesPoolPolicy

描述：將許可授予 Application Auto Scaling 以存取 Amazon WorkSpaces 和 Amazon CloudWatch 的政策。

`AWSApplicationAutoscalingWorkSpacesPoolPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 6 月 17 日 18：39 UTC
- 編輯時間：2024 年 6 月 17 日 18：39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesActionsOnAllPools",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspacesPools",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSApplicationDiscoveryAgentAccess

描述：提供 Discovery Agent 向 AWS Application Discovery Service 註冊的存取權。

`AWSApplicationDiscoveryAgentAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationDiscoveryAgentAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2016 年 5 月 11 日 21：38 UTC
- 編輯時間：2020 年 2 月 24 日，22：26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationDiscoveryAgentlessCollectorAccess

描述：允許 Application Discovery Service 無代理程式收集器自動更新、註冊並與 Application Discovery Service 通訊

`AWSApplicationDiscoveryAgentlessCollectorAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSApplicationDiscoveryAgentlessCollectorAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 8 月 16 日 21：00 UTC
- 編輯時間：2022 年 8 月 16 日 21：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationDiscoveryServiceFullAccess

描述：提供檢視和標記 AWS Application Discovery Service 維護之組態項目的完整存取權

`AWSApplicationDiscoveryServiceFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationDiscoveryServiceFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 5 月 11 日 21：30 UTC
- 編輯時間：2019 年 6 月 19 日 21：21 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationAgentInstallationPolicy

描述：此政策允許安裝 AWS 複寫代理程式，此代理程式會與 AWS Application Migration Service (MGN) 搭配使用，以將外部伺服器遷移至其中 AWS。將此政策連接至您在安裝複寫代理程式時提供憑證的 IAM AWS 使用者或角色。

`AWSApplicationMigrationAgentInstallationPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationMigrationAgentInstallationPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 6 月 19 日 07：51 UTC
- 編輯時間：2022 年 9 月 20 日 11：21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSApplicationMigrationAgentPolicy

描述：此政策允許安裝和使用 AWS Replication Agent，其會與 AWS Application Migration Service (MGN) 搭配使用，以將外部伺服器遷移至 AWS。將此政策連接至您在安裝複寫代理程式時提供憑證的 IAM AWS 使用者或角色。

`AWSApplicationMigrationAgentPolicy` 是 AWS 受管政策。

使用此政策

您可以將 AWSApplicationMigrationAgentPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 4 月 7 日，UTC 07：00
- 編輯時間：2022 年 9 月 20 日 11：13 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationAgentPolicy_v2

描述：此政策允許使用 AWS 複寫代理程式，此代理程式與 AWS Application Migration Service (MGN) 搭配使用，以將外部伺服器遷移至 AWS。我們不建議您將此政策連接至 IAM 使用者或角色。

AWSApplicationMigrationAgentPolicy_v2 是 AWS 受管政策。

使用此政策

您可以將 AWSApplicationMigrationAgentPolicy_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 6 月 6 日 14：14 UTC

- **編輯時間**：2022 年 6 月 6 日 14：14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationConversionServerPolicy

描述：此政策允許 Application Migration Service (MGN) Conversion Server，這是 Application Migration Service 啟動的 EC2 執行個體，可與 MGN 服務通訊。具有此政策的 IAM 角色會由 MGN 連接至 MGN 轉換伺服器（做為 EC2 執行個體設定檔），並在需要時由 MGN 自動啟動和終止。我們不建議您將此政策連接至 IAM 使用者或角色。當使用者選擇使用 MGN 主控台、CLI 或 API 啟動測試或切換執行個體時，Application Migration Service 會使用 MGN 轉換伺服器。

`AWSApplicationMigrationConversionServerPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationMigrationConversionServerPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 4 月 7 日，UTC 06：48
- 編輯時間：2021 年 4 月 7 日 06：48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSApplicationMigrationEC2Access

描述：此政策提供使用 Application Migration Service (MGN) 啟動遷移伺服器做為 EC2 執行個體所需的 Amazon EC2 EC2 操作。將此政策連接至您的 IAM 使用者或角色。

`AWSApplicationMigrationEC2Access` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationMigrationEC2Access` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 4 月 7 日，UTC 07：05
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*",
        "arn:aws:ec2:*:*:network-interface/*"
```

```
      ],
      "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"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationFullAccess

描述：此政策提供 AWS Application Migration Service (MGN) 所有公有 APIs的許可，以及讀取 KMS 金鑰資訊的許可。將此政策連接至您的 IAM 使用者或角色。

`AWSApplicationMigrationFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationMigrationFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 4 月 7 日，UTC 06：56
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
```

```
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Sid" : "VisualEditor14",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor15",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Sid" : "VisualEditor16",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Sid" : "VisualEditor17",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "VisualEditor18",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSMigration-*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor19",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor20",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationMGHAccess

描述：此政策允許 AWS Application Migration Service (MGN) 傳送使用 MGN 遷移至 AWS Migration Hub (MGH) 之伺服器進度的中繼資料。MGN 會自動建立已連接此政策的 IAM 角色，並擔任此角色。我們不建議您將此政策連接至 IAM 使用者或角色。

`AWSApplicationMigrationMGHAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationMigrationMGHAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 4 月 7 日 07：10 UTC
- 編輯時間：2021 年 4 月 7 日 07：10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationNetworkMigrationCustomResource

描述：提供 Network Migration 自訂資源的許可

AWSApplicationMigrationNetworkMigrationCustomResource 是 AWS 受管政策。

使用此政策

您可以將 AWSApplicationMigrationNetworkMigrationCustomResource 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 5 日 11：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationCustomResource`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ModifyTGW",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationNetworkMigrationMultiAccount

描述：提供透過 CloudFormation 自動化 VMware 至 AWS 網路基礎設施遷移的許可

AWSApplicationMigrationNetworkMigrationMultiAccount 是 AWS 受管政策。

使用此政策

您可以將 AWSApplicationMigrationNetworkMigrationMultiAccount 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 10 日 09：04 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationMultiAccount

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Sid" : "EC2CFNReadonlyPrefixList",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:prefix-list/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkAnalyzer",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreatePermissionsByCFNNACL",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFNNACLSN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CFNReadonly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
```

```
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MGNCFNDescribe",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:ListStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*"
    },
    {
      "Sid" : "CFNCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2PutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
```

```
      "Sid" : "AnalyzerEC2ResourceSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2RequestSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2SecurityGroupTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
```

```
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "EC2TagCFNSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "CreatePermissionsByResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateNatGateway",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateTGWVpcAttachmentSameOrg",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CFNProvisionNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateVpc",
        "ec2:CreateTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:transit-gateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateSubnet",
```

```
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagRouting",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNAT",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTGWAttachment",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "DeleteENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagInsights",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-insights-path/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2TagCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
```

```
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateTransitGatewayVpcAttachment",
            "CreateTransitGatewayRouteTableAnnouncement",
            "CreateTransitGatewayRouteTable",
            "CreateTransitGatewayRoute",
            "CreateTransitGatewayPrefixListReference",
            "CreateTransitGatewayPolicyTable",
            "CreateTransitGatewayPeeringAttachment",
            "CreateTransitGatewayConnectPeer",
            "CreateTransitGatewayConnect",
            "CreateTransitGateway",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateSubnet",
            "CreateNetworkAcl",
            "CreateRouteTable",
            "CreateNetworkInterface",
            "CreateNetworkInsightsPath",
            "CreateNetworkInsightsAccessScope",
            "CreateLaunchTemplate",
            "AllocateAddress",
            "StartNetworkInsightsAnalysis",
            "CreateVpc"
          ]
        }
      }
    },
    {
      "Sid" : "deployerWorkload",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "putParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "deleteParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:PutResourcePolicy",
        "ssm:DeleteResourcePolicy",
        "ssm:ListTagsForResource",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ramTAgReource",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateResourceShareTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "Bool" : {
          "ram:RequestedAllowsExternalPrincipals" : "false"
        }
      }
    },
    {
      "Sid" : "AssociateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "ram:RequestedResourceType" : [
            "ec2:TransitGateway",
            "ssm:Parameter"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateResourceShareWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGetResourceShares",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*"
    },
    {
      "Sid" : "CreateCustomResourceLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/network-migration-modify-tgw*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OperationsCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassGetRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "PassRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OperationsRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AttachCustomResourceRole",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/
AWSApplicationMigrationNetworkMigrationCustomResource"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MGNCFNBasedResourcesProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateNatGatewayAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSubnet",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateNatGatewayAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyLaunchTemplate",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:ModifyVolume",
        "ec2:ModifyVpcAttribute",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AnalyzerENIResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
```

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSApplicationMigrationReadOnlyAccess

描述：此政策提供 Application Migration Service (MGN) 所有唯讀公有 APIs 的許可，以及一些其他 AWS 服務所需的唯讀 APIs，以便完整使用 MGN 主控台。將此政策連接至您的 IAM 使用者或角色。

`AWSApplicationMigrationReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationMigrationReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 4 月 7 日，UTC 07：15
- 編輯時間：2023 年 3 月 20 日 08：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationReplicationServerPolicy

描述：此政策允許 Application Migration Service (MGN) 複寫伺服器，這是 Application Migration Service 啟動的 EC2 執行個體，可與 MGN 服務通訊，並在您的 中建立 EBS 快照 AWS 帳戶。Application Migration Service 會將具有此政策的 IAM 角色（做為 EC2 執行個體設定檔）連接至 MGN 複寫伺服器，該伺服器會視需要由 MGN 自動啟動和終止。MGN 複寫伺服器用於促進從外部伺服器到 的資料複寫 AWS，作為使用 MGN 管理的遷移程序的一部分。我們不建議您將此政策連接至 IAM 使用者或角色。

`AWSApplicationMigrationReplicationServerPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationMigrationReplicationServerPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 4 月 7 日，UTC 07：21
- 編輯時間：2021 年 4 月 7 日 07：21 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationServiceEc2InstancePolicy

描述：此政策允許安裝和使用 AWS 複寫代理程式， AWS Application Migration Service (AWS MGN) 使用它來遷移在 EC2 （跨區域或跨可用區域） 上執行的來源伺服器。具有此政策的 IAM 角色應附加 （做為 EC2 執行個體描述檔） 至 EC2 執行個體。

`AWSApplicationMigrationServiceEc2InstancePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSApplicationMigrationServiceEc2InstancePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 8 月 22 日 13：19 UTC
- 編輯時間：2024 年 1 月 3 日 14：19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationServiceRolePolicy

描述：允許 AWS 應用程式 Migration Service 代表您建立和管理 AWS 資源。

AWSApplicationMigrationServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 4 月 7 日，UTC 06：43
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationSSMAccess

描述：此政策提供使用 Application Migration Service (MGN) 執行自訂遷移後命令 SSM 文件所需的 Amazon SSM 操作存取權。將此政策連接至您的 IAM 使用者或角色。

AWSApplicationMigrationSSMAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSApplicationMigrationSSMAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 11 月 27 日 09：29 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSApplicationMigrationVCenterClientPolicy

描述：此政策允許安裝和使用與 AWS Application Migration Service (MGN) 搭配使用的 AWS VCenter 用戶端，以將外部伺服器遷移至其中 AWS。將此政策連接至您在安裝 AWS VCenter 用戶端時提供憑證的 IAM 使用者或角色。

AWSApplicationMigrationVCenterClientPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSApplicationMigrationVCenterClientPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 8 日 12：53 UTC
- 編輯時間：2021 年 11 月 8 日 12：53 UTC
- ARN: arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppMeshEnvoyAccess

描述：用於存取虛擬節點組態的 App Mesh Envoy 政策。

AWSAppMeshEnvoyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAppMeshEnvoyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 7 月 3 日 21：29 UTC
- 編輯時間：2019 年 7 月 3 日 21：29 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppMeshFullAccess

描述：提供 AWS App Mesh APIs和管理主控台的完整存取權。

`AWSAppMeshFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSAppMeshFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2019 年 4 月 16 日 17：50 UTC
- **編輯時間**：2021 年 1 月 7 日 19：54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppMeshPreviewEnvoyAccess

描述：用於存取虛擬節點組態的 App Mesh Preview Envoy 政策。

AWSAppMeshPreviewEnvoyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAppMeshPreviewEnvoyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 8 月 5 日 23：32 UTC
- 編輯時間：2019 年 8 月 5 日 23：32 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSAppMeshPreviewServiceRolePolicy

描述：允許存取 AWS 服務 和 AWS App Mesh 使用或管理的資源

AWSAppMeshPreviewServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 6 月 19 日 19：07 UTC
- 編輯時間：2019 年 8 月 21 日，UTC 21：06
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppMeshReadOnly

描述：提供對 AWS App Mesh APIs唯讀存取權。

AWSAppMeshReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSAppMeshReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 4 月 16 日 17：51 UTC
- 編輯時間：2021 年 1 月 7 日 19：53 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppMeshReadOnly

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppMeshServiceRolePolicy

描述：啟用存取 AWS 服務 和 AWS AppMesh 使用或管理的資源

AWSAppMeshServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 6 月 3 日 18：30 UTC
- 編輯時間：2023 年 10 月 10 日 16：46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppRunnerFullAccess

描述：授予所有 App Runner 動作的許可。

AWSAppRunnerFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAppRunnerFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 1 月 11 日 04：02 UTC
- 編輯時間：2022 年 1 月 11 日 04：02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppRunnerReadOnlyAccess

描述：授予許可，以列出和檢視 App Runner 資源的詳細資訊。

AWSAppRunnerReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAppRunnerReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 2 月 24 日 21：24 UTC
- 編輯時間：2022 年 2 月 24 日 21：24 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppRunnerServicePolicyForECRAccess

Description： AWS App Runner 服務政策，將讀取許可授予客戶帳戶中的 Amazon ECR 資源。在建立或更新 App Runner 服務時傳遞給 App Runner 的角色中使用它。

AWSAppRunnerServicePolicyForECRAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAppRunnerServicePolicyForECRAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 5 月 14 日，UTC 19：17
- 編輯時間：2021 年 5 月 14 日 19：17 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSAppSyncAdministrator

描述：提供 AppSync 服務的管理存取權，但不足以透過主控台存取。

AWSAppSyncAdministrator 是 AWS 受管政策。

使用此政策

您可以將 AWSAppSyncAdministrator 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 3 月 20 日 21：20 UTC
- 編輯時間：2019 年 11 月 4 日 19：23 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncAdministrator

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSAppSyncInvokeFullAccess

描述：透過主控台和獨立提供 AppSync 服務的完整調用存取

AWSAppSyncInvokeFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAppSyncInvokeFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 3 月 20 日 21：21 UTC
- 編輯時間：2018 年 3 月 20 日，UTC 21：21
- ARN: arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppSyncPushToCloudWatchLogs

描述：允許 AppSync 將日誌推送至使用者的 CloudWatch 帳戶。

AWSAppSyncPushToCloudWatchLogs 是 AWS 受管政策。

使用此政策

您可以將 AWSAppSyncPushToCloudWatchLogs 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 4 月 9 日 19：38 UTC
- 編輯時間：2018 年 4 月 9 日 19：38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppSyncSchemaAuthor

描述：提供建立、更新和查詢結構描述的存取權。

AWSAppSyncSchemaAuthor 是 AWS 受管政策。

使用此政策

您可以將 AWSAppSyncSchemaAuthor 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 3 月 20 日 21：21 UTC
- 編輯時間：2023 年 2 月 1 日 18：36 UTC
- ARN: arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAppSyncServiceRolePolicy

描述：允許存取 AppSync 使用或管理 AWS 的服務和資源

AWSAppSyncServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 1 月 21 日 19：56 UTC
- 編輯時間：2020 年 1 月 21 日 19：56 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSArtifactAccountSync

描述：允許 AWS Artifact 唯讀存取 AWS Organizations 中的操作。

AWSArtifactAccountSync 是 AWS 受管政策。

使用此政策

您可以將 AWSArtifactAccountSync 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 4 月 10 日，UTC 23：04
- 編輯時間：2018 年 4 月 10 日，UTC 23：04
- ARN: arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSArtifactAgreementsFullAccess

描述：此政策授予列出、下載、接受和終止 AWS Artifact 協議的完整許可。它還包含列出和啟用 Organization AWS 服務中服務存取的許可，以及描述組織詳細資訊的許可。此外，該政策提供檢查所需服務連結角色是否存在的能力，並在其不存在時建立一個

`AWSArtifactAgreementsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSArtifactAgreementsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 11 月 22 日 19：36 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSArtifactAgreementsFullAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource" : "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid" : "CustomerAgreementActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRoleToCheckForRoleExistence",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid" : "EnableServiceTrust",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EnableServiceTrustForArtifact",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "aws-artifact-account-sync.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSArtifactAgreementsReadOnlyAccess

描述：此政策授予唯讀存取權，以列出 AWS Artifact 服務協議並下載接受的協議。它還包含列出和描述組織詳細資訊的許可。此外，政策提供檢查所需服務連結角色是否存在的能力。

`AWSArtifactAgreementsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSArtifactAgreementsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- **建立時間**：2024 年 11 月 22 日 19：36 UTC
- **編輯時間**：2026 年 2 月 12 日 18：00 UTC

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

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementsActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetCustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "AWSOrganizationActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRole",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSArtifactReportsReadOnlyAccess

描述：提供 AWS Artifact 服務報告的唯讀存取權。

`AWSArtifactReportsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSArtifactReportsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 1 月 2 日 22：42 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "artifact:ListReportVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSArtifactServiceRolePolicy

描述：允許 AWS Artifact 透過 AWS Organizations 服務收集有關組織的資訊。

`AWSArtifactServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 8 月 21 日 20：27 UTC
- 編輯時間：2023 年 8 月 21 日 20：27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSAuditManagerAdministratorAccess

描述：提供啟用或停用 AWS Audit Manager、更新設定和管理評估、控制項和架構的管理存取權

AWSAuditManagerAdministratorAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSAuditManagerAdministratorAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 11 日 20：02 UTC
- 編輯時間：2024 年 5 月 15 日 23：46 UTC
- ARN: arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "auditmanager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "auditmanager.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMAccessManageSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:UpdateRoleDescription",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
```

```
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ControlCatalogAccess",
      "Effect" : "Allow",
      "Action" : [
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSAuditManagerServiceRolePolicy

描述：允許存取 AWS Audit Manager 使用或管理的 AWS 服務 和 資源

AWSAuditManagerServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 8 日 15：12 UTC
- 編輯時間：2024 年 9 月 24 日 23：22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
```

```
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:GetLaunchTemplateData",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccessKeyLastUsed",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
```

```
            "iam:ListGroupsForUser",
            "iam:ListGroupPolicies",
            "iam:ListGroups",
            "iam:ListOpenIdConnectProviders",
            "iam:ListPolicies",
            "iam:ListRolePolicies",
            "iam:ListRoles",
            "iam:ListSamlProviders",
            "iam:ListUserPolicies",
            "iam:ListUsers",
            "iam:ListVirtualMFADevices",
            "iam:ListPolicyVersions",
            "iam:ListAccessKeys",
            "iam:ListAttachedRolePolicies",
            "iam:ListMfaDeviceTags",
            "iam:ListMfaDevices",
            "kafka:ListClusters",
            "kafka:ListKafkaVersions",
            "kinesis:ListStreams",
            "kms:DescribeKey",
            "kms:GetKeyPolicy",
            "kms:GetKeyRotationStatus",
            "kms:ListGrants",
            "kms:ListKeyPolicies",
            "kms:ListKeys",
            "lambda:ListFunctions",
            "license-manager:ListAssociationsForLicenseConfiguration",
            "license-manager:ListLicenseConfigurations",
            "license-manager:ListUsageForLicenseConfiguration",
            "logs:DescribeDestinations",
            "logs:DescribeExportTasks",
            "logs:DescribeLogGroups",
            "logs:DescribeMetricFilters",
            "logs:DescribeResourcePolicies",
            "logs:FilterLogEvents",
            "logs:GetDataProtectionPolicy",
            "es:DescribeDomains",
            "es:DescribeDomain",
            "es:DescribeDomainConfig",
            "es:ListDomainNames",
            "organizations:DescribeOrganization",
            "organizations:DescribePolicy",
            "rds:DescribeCertificates",
            "rds:DescribeDBClusterEndpoints",
```

```
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeLoggingStatus",
        "route53:GetQueryLoggingConfig",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListModels",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListUserProfiles",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
```

```
        "securityhub:DescribeStandards",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetRule",
        "waf-regional:GetWebAcl",
        "waf:GetRule",
        "waf:GetRuleGroup",
        "waf:ListActivatedRulesInRuleGroup",
        "waf:ListWebAcls",
        "wafv2:ListWebAcls",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf-regional:ListRules",
        "waf:ListRuleGroups",
        "waf:ListRules"
      ],
      "Resource" : "*",
      "Sid" : "APIsAccess"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLogging",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:source" : "false"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
```

```
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSAutoScalingPlansEC2AutoScalingPolicy

描述：將許可授予 AWS Auto Scaling 以定期預測容量並在擴展計畫中為 Auto Scaling 群組產生排程擴展動作的政策

AWSAutoScalingPlansEC2AutoScalingPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 8 月 23 日，UTC 22：46
- 編輯時間：2018 年 8 月 23 日，UTC 22：46
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSBackupAuditAccess

描述：此政策授予許可，讓使用者建立控制和架構，以定義他們對 AWS 備份資源和活動的期望，並根據其定義的控制和架構稽核 AWS 備份資源和活動。此政策會授予 Config AWS 和類似服務的許可，以描述使用者執行稽核的期望。此政策也會授予許可，以將稽核報告交付至 S3 和類似服務，並讓使用者尋找和開啟其稽核報告。

AWSBackupAuditAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupAuditAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 8 月 24 日 01：02 UTC
- 編輯時間：2023 年 4 月 10 日 21：23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBackupDataTransferAccess

描述：此政策允許 AWS Backint 代理程式使用 Backup Storage 平面完成 AWS 備份資料傳輸。將此政策連接至執行 SAP HANA 的 EC2 執行個體與 Backint 代理程式所擔任的角色。

`AWSBackupDataTransferAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupDataTransferAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 10 日 22：48 UTC
- 編輯時間：2022 年 11 月 10 日 22：48 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupDataTransferAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBackupFullAccess

描述：此政策適用於備份管理員，授予 AWS 備份操作的完整存取權，包括建立或編輯備份計劃、將 AWS 資源指派給備份計劃、刪除備份和還原備份。

AWSBackupFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 11 月 18 日 22：21 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupFullAccess

政策版本

政策版本： v30 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayGatewayStarPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "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" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeletetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "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" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

描述：Provide AWS BackupGateway 代表您同步虛擬機器中繼資料的許可

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 12 月 15 日 19：43 UTC
- 編輯時間：2022 年 12 月 15 日 19：43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupGuardDutyRolePolicyForScans

描述：提供 GuardDuty 許可，以讀取 AWS 備份復原點以進行惡意軟體掃描

AWSBackupGuardDutyRolePolicyForScans 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupGuardDutyRolePolicyForScans 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 20 日 03：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupGuardDutyRolePolicyForScans

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "CreateGrantForEncryptedVolumeCreation",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:guardduty:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
```

```
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "CreateGrantForReEncryptAndEBSDirect",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ShareSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : [
            "vol-*",
            "snap-*"
          ],
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBackupAccessPointPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "backup:CreateBackupAccessPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "ReadAndDeleteBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupAccessPoint",
        "backup:DeleteBackupAccessPoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupRecoveryPointApiPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "DecryptKMSEncryptedDataByAWSBackup",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:backup:backup-vault" : "*",
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupOperatorAccess

描述：此政策授予使用者將 AWS 資源指派給備份計畫的許可、建立隨需備份和還原備份。此政策不允許使用者建立或編輯備份計畫，或在建立排程備份後刪除排程備份。

AWSBackupOperatorAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupOperatorAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 11 月 18 日 22：23 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOperatorAccess

政策版本

政策版本： v28 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
```

```
        "backup:Describe*",
        "backup:CreateBackupSelection",
        "backup:DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob",
        "backup:StartScanJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeAccess",
      "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" : "DynamoDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
```

```
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EC2Access",
      "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" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewaySCSIAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayReadAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayDiskReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayVolumeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMComandAccess",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FSXDescribeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FSxFileAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FSxVolumeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*"
    },
```

```
    {
      "Sid" : "FSxMachineAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeStorageVirtualMachines",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Sid" : "DirectoryServiceAccess",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayListAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayMachineAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamListAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftAccess",
      "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" : "RedshiftOptionsAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
```

```
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "CloudFormationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SAPAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SAPDatabaseAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
```

```
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupOrganizationAdminAccess

描述：此政策適用於使用跨帳戶備份管理來管理組織的備份的備份管理員。

AWSBackupOrganizationAdminAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupOrganizationAdminAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 6 月 24 日 16：23 UTC
- 編輯時間：2022 年 11 月 18 日 18：26 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupRestoreAccessForSAPHANA

描述：提供 AWS 備份許可，以還原 Amazon EC2 上的 SAP HANA 備份

AWSBackupRestoreAccessForSAPHANA 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupRestoreAccessForSAPHANA 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2022 年 11 月 10 日，UTC 22：43
- **編輯時間**：2022 年 11 月 10 日 22：43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupSearchOperatorAccess

描述：搜尋運算子角色有權建立備份索引、建立已編製索引之備份中繼資料的搜尋。此政策包含這些搜尋運算子函數的必要許可。

AWSBackupSearchOperatorAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupSearchOperatorAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 2 月 27 日 21：52 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupSearchOperatorAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartSearchAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchJob",
        "backup-search:ListSearchJobs",
        "backup-search:ListSearchResultExportJobs",
        "backup:ListIndexedRecoveryPointsForSearch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupSearchRecoveryPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:SearchRecoveryPoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:backup:*:*:recovery-point:*"
      ]
    },
    {
      "Sid" : "SearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchResultExportJob",
        "backup-search:StopSearchJob",
        "backup-search:GetSearchJob",
        "backup-search:GetSearchResultExportJob",
        "backup-search:ListSearchJobResults",
        "backup-search:ListSearchJobBackups"
      ],
      "Resource" : [
        "arn:aws:backup-search:*:*:search-job/*",
```

```
        "arn:aws:backup-search:*:*:search-export-job/*"
      ]
    },
    {
      "Sid" : "KMSDataKeyForSearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:backup-search:search-job"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "backup.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBackupServiceLinkedRolePolicyForBackup

描述：提供 AWS 備份許可，以代表您跨 AWS 服務建立備份

AWSBackupServiceLinkedRolePolicyForBackup 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 6 月 2 日 23：08 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

政策版本

政策版本： v31 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSBackupManagedResource"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
```

```
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "RDSInstanceAndSnashotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBSnapshot",
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBInstanceAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSSnapshotTenantDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot-tenant-database:awsbackup:*"
      ]
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CopyBackup",
```

```
        "fsx:TagResource",
        "fsx:DescribeBackups",
        "fsx:DeleteBackup"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
```

```
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeTable",
        "timestream:GetAwsBackupStatus",
```

```
        "timestream:GetAwsRestoreStatus"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
```

```
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeleteSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrgsListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupServiceLinkedRolePolicyForBackupTest

描述：提供 AWS 備份許可，以代表您跨 AWS 服務建立備份

AWSBackupServiceLinkedRolePolicyForBackupTest 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 5 月 12 日 17：37 UTC
- 編輯時間：2020 年 5 月 12 日 17：37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Effect" : "Allow",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Action" : [
```

```
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupServiceRolePolicyForBackup

描述：提供 AWS 備份許可，以代表您跨 AWS 服務建立備份

AWSBackupServiceRolePolicyForBackup 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupServiceRolePolicyForBackup 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 1 月 10 日 21：01 UTC
- 編輯時間：2026 年 2 月 23 日 19：42 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup

政策版本

政策版本： v30 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "RDSInstanceAutomatedBackupPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBInstanceAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:auto-backup:*"
    },
    {
      "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" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "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" : "*"
```

```
    },
    {
      "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" : "KMSEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:ebs:id"
        }
      }
    },
    {
      "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" : "RedshiftServerlessCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*",
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
```

```
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLResourcePermissionsForBackup",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDSQLPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
```

```
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBackupAccessEntry",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "AssociateBackupAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForBackup",
          "eks:accessScope" : "cluster"
        }
      }
    },
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyMalwareScanIAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupServiceRolePolicyForIndexing

描述：政策包含 AWS 備份索引復原點所需的許可。

AWSBackupServiceRolePolicyForIndexing 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupServiceRolePolicyForIndexing 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 17 日 18：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "KMSDataKeyForEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupServiceRolePolicyForItemRestores

描述：政策包含 AWS 備份在復原點中還原個別項目所需的許可

AWSBackupServiceRolePolicyForItemRestores 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupServiceRolePolicyForItemRestores 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 17 日 18：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
```

```
    },
    {
      "Sid" : "S3ReadonlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForFileLevelRestore",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataKeyForS3AndEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "s3.*.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBackupServiceRolePolicyForRestores

描述：提供 AWS 備份許可，以代表您跨 AWS 服務執行還原。此政策包含建立和刪除 AWS 資源的許可，例如 EBS 磁碟區、RDS 執行個體和 EFS 檔案系統，這些都是還原程序的一部分。

`AWSBackupServiceRolePolicyForRestores` 是 AWS 受管政策。

使用此政策

您可以將 `AWSBackupServiceRolePolicyForRestores` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 1 月 12 日 00：23 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

政策版本

政策版本： v35 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "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",
        "rds:CreateTenantDatabase",
        "rds:DeleteTenantDatabase"
      ],
      "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" : "DSQLResourcePermissionsForRestore",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:TagResource",
        "dsql:CreateCluster",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:UpdateCluster",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "dsql.*.amazonaws.com",
            "redshift-serverless.*.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" : {
        "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:*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeTableRestoreStatus"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:RestoreTableFromSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetTableRestoreStatus"
      ],
      "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" : [
        "*"
      ]
    },
    {
      "Sid" : "EKSClusterRestore",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCluster",
        "eks:DescribeCluster",
        "eks:CreateAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:AssociateAccessPolicy",
        "eks:ListAssociatedAccessPolicies",
        "eks:CreateAddon",
        "eks:DescribeAddon",
        "eks:CreateNodegroup",
        "eks:DescribeNodegroup",
        "eks:CreateFargateProfile",
        "eks:DescribeFargateProfile",
        "eks:CreatePodIdentityAssociation",
        "eks:DescribePodIdentityAssociation",
        "eks:TagResource"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:access-entry/*",
        "arn:aws:eks:*:*:addon/*",
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:fargateprofile/*",
        "arn:aws:eks:*:*:nodegroup/*",
        "arn:aws:eks:*:*:podidentityassociation/*"
```

```
      ]
    },
    {
      "Sid" : "AssociateRestoreAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForRestore",
          "eks:accessScope" : "cluster"
        }
      }
    },
    {
      "Sid" : "CreateClusterIAMPerms",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "eks.amazonaws.com",
            "ec2.amazonaws.com",
            "pods.eks.amazonaws.com",
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEKSNodeGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets",
        "ec2:RunInstances",
        "iam:GetRole",
```

```
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSNodeGroupTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "BackupRestoreJobManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:StartRestoreJob",
        "backup:ListRestoreJobs",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:DescribeRestoreJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBackupServiceRolePolicyForS3Backup

描述：政策包含 AWS 備份以備份任何 S3 儲存貯體中的資料所需的許可。這包括所有 S3 物件的讀取存取權，以及所有 KMS 金鑰的任何解密存取權。

AWSBackupServiceRolePolicyForS3Backup 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupServiceRolePolicyForS3Backup 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 2 月 18 日 17：40 UTC
- 編輯時間：2024 年 5 月 17 日 17：12 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchGetMetricDataPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EventBridgePermissionsForAwsBackupManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeListRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:GetInventoryConfiguration",
        "s3:ListBucketVersions",
        "s3:ListBucket",
```

```
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutInventoryConfiguration",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/*"
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListAllMyBuckets",
      "Resource" : "*"
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupServiceRolePolicyForS3Restore

描述：政策包含 AWS 備份將 S3 備份還原至儲存貯體所需的許可。這包括所有 S3 儲存貯體的讀取/寫入許可，以及所有 KMS 金鑰的 GenerateDataKey 和 DescribeKey 許可。

AWSBackupServiceRolePolicyForS3Restore 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupServiceRolePolicyForS3Restore 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 2 月 18 日 17：39 UTC
- 編輯時間：2023 年 2 月 7 日 00：06 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBackupServiceRolePolicyForScans

描述：提供 AWS 備份許可，以在 AWS 備份復原點上執行惡意軟體掃描

AWSBackupServiceRolePolicyForScans 是 AWS 受管政策。

使用此政策

您可以將 AWSBackupServiceRolePolicyForScans 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 11 月 20 日 03：34 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForScans

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBatchFullAccess

描述：提供 AWS Batch 資源的完整存取權。

AWSBatchFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBatchFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 12 月 6 日 19：35 UTC
- 編輯時間：2022 年 10 月 24 日 16：09 UTC
- ARN: arn:aws:iam::aws:policy/AWSBatchFullAccess

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBatchServiceEventTargetRole

描述：為 AWS 批次任務提交啟用 CloudWatch 事件目標的政策

AWSBatchServiceEventTargetRole 是 AWS 受管政策。

使用此政策

您可以將 AWSBatchServiceEventTargetRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 2 月 28 日，22：31 UTC
- 編輯時間：2018 年 2 月 28 日，UTC 22：31
- ARN: arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBatchServiceRole

描述： AWS Batch 服務角色的政策，允許存取相關服務，包括 EC2、Autoscaling、EC2 Container 服務和 Cloudwatch Logs。

`AWSBatchServiceRole` 是 AWS 受管政策。

使用此政策

您可以將 `AWSBatchServiceRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 12 月 6 日 19：36 UTC
- 編輯時間：2023 年 12 月 5 日 18：49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBatchServiceRolePolicyForSageMaker

描述：提供 AWS Batch 佇列和管理 Amazon SageMaker 工作負載的存取權

`AWSBatchServiceRolePolicyForSageMaker` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 7 月 15 日，UTC 21：37
- 編輯時間：2025 年 7 月 15 日 21：37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBatchServiceRolePolicyForSageMaker`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateTrainingJob"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBCMDataExportsServiceRolePolicy

描述：服務連結角色，提供 Billing and Cost Management Data Exports 存取 AWS 服務資料，以代表客戶將資料匯出至目標位置，例如 Amazon S3。

`AWSBCMDataExportsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 6 月 10 日 17：40 UTC
- 編輯時間：2024 年 6 月 10 日 17：40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSBillingConductorFullAccess

描述：使用 AWSBillingConductorFullAccess 受管政策允許完整存取 AWS Billing Conductor (ABC) 主控台和 APIs。此政策允許使用者列出、建立和刪除 ABC 資源。

AWSBillingConductorFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBillingConductorFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 4 月 13 日 18：02 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingConductorFullAccess

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
```

```
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeResponsibilityTransfer",
        "organizations:ListInboundResponsibilityTransfers"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBillingConductorReadOnlyAccess

描述：使用 AWSBillingConductorReadOnlyAccess 受管政策允許唯讀存取 AWS Billing Conductor (ABC) 主控台和 APIs。此政策授予檢視和列出所有 ABC 資源的許可。它不包括建立或刪除資源的功能。

`AWSBillingConductorReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSBillingConductorReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 4 月 13 日 18：02 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "billingconductor:GetBillingGroupCostReport",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBillingReadOnlyAccess

描述：允許使用者在帳單主控台上檢視帳單。

AWSBillingReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBillingReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 8 月 27 日，20：08 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess

政策版本

政策版本： v26 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
```

```
            "billing:GetContractInformation",
            "billing:GetIAMAccessPreference",
            "billing:GetSellerOfRecord",
            "billing:ListBillingViews",
            "budgets:ViewBudget",
            "budgets:DescribeBudgetActionsForBudget",
            "budgets:DescribeBudgetAction",
            "budgets:DescribeBudgetActionsForAccount",
            "budgets:DescribeBudgetActionHistories",
            "ce:DescribeCostCategoryDefinition",
            "ce:GetCostAndUsage",
            "ce:ListCostCategoryDefinitions",
            "ce:ListTagsForResource",
            "ce:ListCostAllocationTags",
            "ce:ListCostAllocationTagBackfillHistory",
            "ce:GetTags",
            "ce:GetDimensionValues",
            "ce:GetCostAndUsageComparisons",
            "ce:GetCostComparisonDrivers",
            "consolidatedbilling:ListLinkedAccounts",
            "consolidatedbilling:GetAccountBillingRole",
            "cur:GetClassicReport",
            "cur:GetClassicReportPreferences",
            "cur:GetUsageReport",
            "cur:DescribeReportDefinitions",
            "freetier:GetFreeTierAlertPreference",
            "freetier:GetFreeTierUsage",
            "freetier:GetAccountPlanState",
            "freetier:GetAccountActivity",
            "freetier:ListAccountActivities",
            "invoicing:BatchGetInvoiceProfile",
            "invoicing:GetInvoiceEmailDeliveryPreferences",
            "invoicing:GetInvoicePDF",
            "invoicing:GetInvoiceUnit",
            "invoicing:GetInvoiceCorrection",
            "invoicing:ListInvoiceSummaries",
            "invoicing:ListInvoiceUnits",
            "invoicing:GetProcurementPortalPreference",
            "invoicing:ListProcurementPortalPreferences",
            "invoicing:ListTagsForResource",
            "invoicing:ListInvoiceCorrections",
            "mapcredits:ListQuarterSpend",
            "mapcredits:ListAssociatedPrograms",
            "mapcredits:ListQuarterCredits",
```

```
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBillingServiceRolePolicy

描述：允許帳單服務驗證對衍生帳單檢視之帳單檢視資料的存取

AWSBillingServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 9 月 11 日 16：19 UTC
- 編輯時間：2025 年 9 月 11 日 16：19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

描述：此政策提供控制 AWS 資源的許可。例如，透過執行 AWS Systems Manager (SSM) 指令碼來啟動和停止 EC2 或 RDS 執行個體。

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 是 AWS 受管政策。

使用此政策

您可以將 AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 5 月 25 日 19：03 UTC
- 編輯時間：2022 年 5 月 25 日 19：03 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBudgetsActionsWithAWSResourceControlAccess

描述：提供 AWS Budgets 動作的完整存取權，包括使用 Budgets 動作透過 控制執行中 AWS 資源的狀態 AWS 管理主控台

AWSBudgetsActionsWithAWSResourceControlAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBudgetsActionsWithAWSResourceControlAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 10 月 15 日 17：19 UTC
- 編輯時間：2020 年 10 月 15 日 17：19 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
        "ec2:DescribeInstances",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListPolicies",
        "organizations:ListRoots",
        "rds:DescribeDBInstances",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBudgetsReadOnlyAccess

描述：透過 提供對 AWS Budgets Console 的唯讀存取權 AWS 管理主控台。

AWSBudgetsReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBudgetsReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 10 月 15 日 17：18 UTC
- 編輯時間：2024 年 6 月 17 日 17：41 UTC
- ARN: arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSBugBustFullAccess

描述：此 IAM 政策授予使用者對 AWS BugBust 主控台的完整存取權

`AWSBugBustFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSBugBustFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 6 月 24 日 07：03 UTC
- 編輯時間：2021 年 7 月 22 日，UTC 20：04
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBugBustPlayerAccess

描述：此 IAM 政策授予使用者參與 in AWS BugBust 事件的存取權

AWSBugBustPlayerAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSBugBustPlayerAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 6 月 24 日 07：15 UTC
- 編輯時間：2021 年 6 月 24 日 07：15 UTC
- ARN: arn:aws:iam::aws:policy/AWSBugBustPlayerAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSBugBustServiceRolePolicy

描述：授予許可給 AWS BugBust 以代表您存取資源

AWSBugBustServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 6 月 24 日 06：59 UTC
- 編輯時間：2021 年 6 月 24 日 06：59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCertificateManagerFullAccess

描述：提供 AWS Certificate Manager (ACM) 的完整存取權

`AWSCertificateManagerFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCertificateManagerFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2016 年 1 月 21 日 17：02 UTC
- 編輯時間：2020 年 8 月 17 日 22：18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCertificateManagerPrivateCAAuditor

描述：提供稽核人員對 AWS Certificate Manager Private Certificate Authority 的存取權

AWSCertificateManagerPrivateCAAuditor 是 AWS 受管政策。

使用此政策

您可以將 AWSCertificateManagerPrivateCAAuditor 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 10 月 23 日 16：51 UTC
- 編輯時間：2020 年 8 月 17 日，UTC 22：54
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCertificateManagerPrivateCAFullAccess

描述：提供 AWS Certificate Manager Private Certificate Authority 的完整存取權

`AWSCertificateManagerPrivateCAFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCertificateManagerPrivateCAFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2018 年 10 月 23 日 16：54 UTC
- 編輯時間：2018 年 10 月 23 日 16：54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCertificateManagerPrivateCAPrivilegedUser

描述：提供對 AWS Certificate Manager Private Certificate Authority 的特權憑證使用者存取權

`AWSCertificateManagerPrivateCAPrivilegedUser` 是 AWS 受管政策。

使用此政策

您可以將 AWSCertificateManagerPrivateCAPrivilegedUser 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 6 月 20 日 17：43 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
```

```
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCertificateManagerPrivateCAReadOnly

描述：提供 AWS Certificate Manager Private Certificate Authority 的唯讀存取權

AWSCertificateManagerPrivateCAReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSCertificateManagerPrivateCAReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 10 月 23 日 16：57 UTC
- 編輯時間：2020 年 8 月 17 日，UTC 22：54
- ARN: arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCertificateManagerPrivateCAUser

描述：提供憑證使用者對 AWS Certificate Manager Private Certificate Authority 的存取權

`AWSCertificateManagerPrivateCAUser` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCertificateManagerPrivateCAUser` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 10 月 23 日 16：53 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "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" : "*"
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCertificateManagerReadOnly

描述：提供 AWS Certificate Manager (ACM) 的唯讀存取權。

`AWSCertificateManagerReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCertificateManagerReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 1 月 21 日 17：07 UTC
- 編輯時間：2021 年 3 月 15 日 16：25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSChatbotServiceLinkedRolePolicy

描述： AWS Chatbot 使用的服務連結角色。

AWSChatbotServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 18 日 16：39 UTC
- 編輯時間：2019 年 11 月 18 日 16：39 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSCleanRoomsFullAccess

描述：允許完整存取 AWS Clean Rooms 資源和存取相關 AWS 服務。

AWSCleanRoomsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCleanRoomsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 1 月 12 日 16：10 UTC
- 編輯時間：2024 年 3 月 21 日 15：35 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCleanRoomsFullAccessNoQuerying

描述：允許完整存取 AWS Clean Rooms 資源，但協同合作中查詢和存取相關資源除外 AWS 服務。

AWSCleanRoomsFullAccessNoQuerying 是 AWS 受管政策。

使用此政策

您可以將 AWSCleanRoomsFullAccessNoQuerying 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 1 月 12 日 16：12 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableReference",
        "cleanrooms:UpdateConfiguredTableAllowedColumns",
        "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCleanRoomsMLFullAccess

描述：允許完整存取 AWS Clean Rooms ML 資源和存取相關資源 AWS 服務。

AWSCleanRoomsMLFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCleanRoomsMLFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 11 月 29 日 21：02 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:BatchGetSchema",
        "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*"
    },
    {
      "Sid" : "ConsoleDescribeECRRepositories",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:ListImages"
```

```
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCleanRoomsMLReadOnlyAccess

描述：允許對 AWS Clean Rooms ML 資源的唯讀存取權，以及對相關 AWS Clean Rooms 資源的唯讀存取權

`AWSCleanRoomsMLReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCleanRoomsMLReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 11 月 29 日，UTC 20：55
- 編輯時間：2026 年 2 月 12 日 18：00 UTC

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

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCleanRoomsReadOnlyAccess

描述：允許對 AWS Clean Rooms 資源的唯讀存取權，以及對相關 AWS Glue 和 Amazon CloudWatch Logs 資源的唯讀存取權。

`AWSCleanRoomsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCleanRoomsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 1 月 12 日 16：10 UTC
- 編輯時間：2023 年 1 月 12 日 16：10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCleanRoomsServiceRolePolicy

描述：允許 AWS Clean Rooms 代表您存取其他 AWS 服務，例如 CloudWatch APIs。

`AWSCleanRoomsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 12 月 15 日 17：49 UTC
- 編輯時間：2025 年 12 月 15 日 17：49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCleanRoomsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloud9Administrator

描述：提供 AWS Cloud9 的管理員存取權。

AWSCloud9Administrator 是 AWS 受管政策。

使用此政策

您可以將 AWSCloud9Administrator 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 11 月 30 日 16：17 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9Administrator

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloud9EnvironmentMember

描述：提供邀請至 AWS Cloud9 共用開發環境的功能。

`AWSCloud9EnvironmentMember` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCloud9EnvironmentMember` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 30 日 16：18 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "cloud9:GetMigrationExperiences",
        "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/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCloud9ServiceRolePolicy

描述： AWS Cloud9 的服務連結角色政策

AWSCloud9ServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- 建立時間：2017 年 11 月 30 日 13：44 UTC
- 編輯時間：2022 年 1 月 17 日 14：06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloud9SSMInstanceProfile

描述：此政策將用於連接 InstanceProfile 上的角色，以允許 Cloud9 使用 SSM Session Manager 連線到執行個體

AWSCloud9SSMInstanceProfile 是 AWS 受管政策。

使用此政策

您可以將 AWSCloud9SSMInstanceProfile 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 5 月 14 日 11：40 UTC
- 編輯時間：2020 年 5 月 14 日 11：40 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCloud9User

描述：提供建立 AWS Cloud9 開發環境和管理擁有環境的許可。

AWSCloud9User 是 AWS 受管政策。

使用此政策

您可以將 AWSCloud9User 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 11 月 30 日 16：16 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloud9User

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "cloud9:GetMigrationExperiences",
```

```
        "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/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudFormationFullAccess

描述：提供 AWS CloudFormation 的完整存取權。

`AWSCloudFormationFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCloudFormationFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 7 月 26 日 21：50 UTC
- 編輯時間：2019 年 7 月 26 日 21：50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudFormationReadOnlyAccess

描述：透過 提供 AWS CloudFormation 的存取權 AWS 管理主控台。

`AWSCloudFormationReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCloudFormationReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2015 年 2 月 6 日 18：39 UTC
- **編輯時間**：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:BatchDescribe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudFrontLogger

描述：將 CloudFront Logger 寫入許可授予 CloudWatch Logs。

AWSCloudFrontLogger 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 6 月 12 日 20：15 UTC
- 編輯時間：2019 年 11 月 22 日 19：33 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudFrontVPCOriginServiceRolePolicy

描述：允許 CloudFront 代表您管理 EC2 彈性網路介面和安全群組。

AWSCloudFrontVPCOriginServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 10 月 24 日 17：45 UTC
- 編輯時間：2024 年 10 月 24 日 17：45 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontVPCOriginServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "EC2Action5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled",
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup"
```

```
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSCloudHSMFullAccess

描述：提供所有 CloudHSM 資源的完整存取權。

AWSCloudHSMFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCloudHSMFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC

- **編輯時間**：2015 年 2 月 6 日 18：39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCloudHSMReadOnlyAccess

描述：提供所有 CloudHSM 資源的唯讀存取權。

`AWSCloudHSMReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCloudHSMReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2015 年 2 月 6 日 18：39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudHSMRole

描述： AWS CloudHSM 服務角色的預設政策。

AWSCloudHSMRole 是 AWS 受管政策。

使用此政策

您可以將 AWSCloudHSMRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudMapDiscoverInstanceAccess

描述：提供 AWS 雲端 Map 探索 API 的存取權。

`AWSCloudMapDiscoverInstanceAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCloudMapDiscoverInstanceAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 29 日 00：02 UTC
- 編輯時間：2023 年 9 月 20 日 21：48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCloudMapFullAccess

描述：提供所有 AWS 雲端 映射動作的完整存取權。

AWSCloudMapFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCloudMapFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2018 年 11 月 28 日，UTC 23：57
- **編輯時間**：2020 年 7 月 29 日 19：15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCloudMapReadOnlyAccess

描述：提供所有 AWS 雲端 映射動作的唯讀存取權。

AWSCloudMapReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCloudMapReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 11 月 28 日，UTC 23：45
- 編輯時間：2023 年 9 月 20 日 21：47 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudMapRegisterInstanceAccess

描述：提供 AWS 雲端 Map 動作的註冊者層級存取權。

`AWSCloudMapRegisterInstanceAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCloudMapRegisterInstanceAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 11 月 29 日 00：04 UTC
- 編輯時間：2023 年 9 月 20 日 21：47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudShellFullAccess

描述：授予使用 AWS CloudShell 搭配所有功能

AWSCloudShellFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCloudShellFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 15 日 18：07 UTC
- 編輯時間：2020 年 12 月 15 日 18：07 UTC
- ARN: arn:aws:iam::aws:policy/AWSCloudShellFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudTrail_FullAccess

描述：提供 AWS CloudTrail 的完整存取權。

`AWSCloudTrail_FullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCloudTrail_FullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 10 月 8 日 23：41 UTC
- 編輯時間：2021 年 2 月 22 日 19：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudTrail_ReadOnlyAccess

描述：提供 AWS CloudTrail 的唯讀存取權。

`AWSCloudTrail_ReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCloudTrail_ReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2022 年 6 月 14 日 17：19 UTC
- **編輯時間**：2022 年 6 月 14 日 17：19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

描述：此政策由名為 AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents 的服務連結角色使用。當 CloudWatch 警示進入 ALARM 狀態時，CloudWatch 會使用此服務連結角色來執行 AWS System Manager Incident Manager 動作。此政策授予代表您啟動事件的許可。

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 4 月 27 日 13：30 UTC
- 編輯時間：2021 年 4 月 27 日 13：30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeArtifactAdminAccess

描述：透過 提供 AWS CodeArtifact 的完整存取權 AWS 管理主控台。

`AWSCodeArtifactAdminAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodeArtifactAdminAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 6 月 16 日 23：53 UTC
- 編輯時間：2020 年 6 月 16 日 23：53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeArtifactReadOnlyAccess

描述：透過 提供 AWS CodeArtifact 的唯讀存取權 AWS 管理主控台。

`AWSCodeArtifactReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodeArtifactReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 6 月 25 日，UTC 21：23

- **編輯時間**：2020 年 6 月 25 日，UTC 21：23
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCodeBuildAdminAccess

描述：透過 提供 AWS CodeBuild 的完整存取權 AWS 管理主控台。同時連接 AmazonS3ReadOnlyAccess 以提供下載建置成品的存取權，並連接 IAMFullAccess 以建立和管理 CodeBuild 的服務角色。

AWSCodeBuildAdminAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeBuildAdminAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 12 月 1 日 19：04 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess

政策版本

政策版本： v20 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "SSMOpenDataChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCodeBuildDeveloperAccess

描述：透過 提供 AWS CodeBuild 的存取權 AWS 管理主控台，但不允許 CodeBuild 專案管理。同時連接 AmazonS3ReadOnlyAccess，以提供下載建置成品的存取權。

`AWSCodeBuildDeveloperAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodeBuildDeveloperAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 12 月 1 日 19：02 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

政策版本

政策版本： v21 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "SSMOpenDataChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "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"
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCodeBuildReadOnlyAccess

描述：透過 提供 AWS CodeBuild 的唯讀存取權 AWS 管理主控台。同時連接 AmazonS3ReadOnlyAccess，以提供下載建置成品的存取權。

AWSCodeBuildReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeBuildReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2016 年 12 月 1 日 19：03 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
```

```
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeCommitFullAccess

描述：透過 提供 AWS CodeCommit 的完整存取權 AWS 管理主控台。

`AWSCodeCommitFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodeCommitFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 7 月 9 日 17：02 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "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/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeCommitPowerUser

描述：提供 AWS CodeCommit 儲存庫的完整存取權，但不允許刪除儲存庫。

`AWSCodeCommitPowerUser` 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeCommitPowerUser 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 7 月 9 日 17：06 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeCommitPowerUser

政策版本

政策版本： v18 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "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/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeCommitReadOnly

描述：透過 提供 AWS CodeCommit 的唯讀存取權 AWS 管理主控台。

`AWSCodeCommitReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodeCommitReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 7 月 9 日 17：05 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCodeDeployDeployerAccess

描述：提供註冊和部署修訂的存取權。

AWSCodeDeployDeployerAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeDeployDeployerAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 5 月 19 日 18：18 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeDeployFullAccess

描述：提供 CodeDeploy 資源的完整存取權。

AWSCodeDeployFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeDeployFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 5 月 19 日 18：13 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployFullAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeDeployReadOnlyAccess

描述：提供 CodeDeploy 資源的唯讀存取權。

`AWSCodeDeployReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodeDeployReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 5 月 19 日 18：21 UTC

- **編輯時間**：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeDeployRole

描述：提供 CodeDeploy 服務存取權，以代表您展開標籤並與 Auto Scaling 互動。

`AWSCodeDeployRole` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodeDeployRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 5 月 4 日 18：05 UTC
- 編輯時間：2023 年 8 月 16 日 20：38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeDeployRoleForCloudFormation

描述：提供 CodeDeploy 服務存取權，以代表您叫用 Lambda 函數，以透過 CloudFormation 執行藍/綠部署。

`AWSCodeDeployRoleForCloudFormation` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodeDeployRoleForCloudFormation` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 5 月 19 日 17：12 UTC
- 編輯時間：2020 年 5 月 19 日 17：12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeDeployRoleForECS

描述：提供 CodeDeploy 服務全存取，以代表您執行 ECS 藍/綠部署。授予支援服務的完整存取權，例如讀取所有 S3 物件的完整存取權、叫用所有 Lambda 函數、發佈至帳戶內的所有 SNS 主題，以及更新所有 ECS 服務。

AWSCodeDeployRoleForECS 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeDeployRoleForECS 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 27 日 20：40 UTC
- 編輯時間：2019 年 9 月 23 日，UTC 22：37
- ARN: arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCodeDeployRoleForECSLimited

描述：提供 CodeDeploy 服務有限的存取權，以代表您執行 ECS 藍/綠部署。

`AWSCodeDeployRoleForECSLimited` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodeDeployRoleForECSLimited` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2018 年 11 月 27 日，UTC 20：42
- **編輯時間**：2019 年 9 月 23 日，UTC 22：10
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeDeployRoleForLambda

描述：提供 CodeDeploy 服務存取權，以代表您執行 Lambda 部署。

AWSCodeDeployRoleForLambda 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeDeployRoleForLambda 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 11 月 28 日 14：05 UTC
- 編輯時間：2019 年 12 月 3 日 19：53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCodeDeployRoleForLambdaLimited

描述：提供 CodeDeploy 服務有限的存取權，以代表您執行 Lambda 部署。

AWSCodeDeployRoleForLambdaLimited 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeDeployRoleForLambdaLimited 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 8 月 17 日 17：14 UTC
- 編輯時間：2020 年 8 月 17 日 17：14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodePipeline_FullAccess

描述：透過 提供 AWS CodePipeline 的完整存取權 AWS 管理主控台。

AWSCodePipeline_FullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCodePipeline_FullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 8 月 3 日，UTC 22：38
- 編輯時間：2024 年 3 月 14 日 17：06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodePipeline_ReadOnlyAccess

描述：透過 提供 AWS CodePipeline 的唯讀存取權 AWS 管理主控台。

`AWSCodePipeline_ReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSCodePipeline_ReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 8 月 3 日，22：25 UTC

- **編輯時間**：2020 年 8 月 3 日，22：25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodePipelineApproverAccess

描述：提供檢視和核准所有管道手動變更的存取權

AWSCodePipelineApproverAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCodePipelineApproverAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 7 月 28 日 18：59 UTC
- 編輯時間：2017 年 8 月 2 日 17：24 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodePipelineCustomActionAccess

描述：提供自訂動作的存取權，以輪詢任務詳細資訊（包括臨時登入資料），並將狀態更新報告給 AWS CodePipeline。

`AWSCodePipelineCustomActionAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSCodePipelineCustomActionAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 7 月 9 日 17：02 UTC
- 編輯時間：2015 年 7 月 9 日 17：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCodeStarFullAccess

描述：透過 提供 AWS CodeStar 的完整存取權 AWS 管理主控台。

AWSCodeStarFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeStarFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 4 月 19 日 16：23 UTC
- 編輯時間：2023 年 3 月 28 日 00：06 UTC
- ARN: arn:aws:iam::aws:policy/AWSCodeStarFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeStarNotificationsServiceRolePolicy

描述：允許 AWS CodeStar Notifications 代表您存取 Amazon CloudWatch Events

`AWSCodeStarNotificationsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 5 日 16：10 UTC
- 編輯時間：2020 年 3 月 19 日 16：01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCodeStarServiceRole

描述：請勿使用 - AWS CodeStar 服務角色政策，授予管理權限，以便 CodeStar 代表客戶管理 IAM 和其他服務資源。

AWSCodeStarServiceRole 是 AWS 受管政策。

使用此政策

您可以將 AWSCodeStarServiceRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 4 月 19 日 15：20 UTC
- 編輯時間：2021 年 9 月 20 日 19：11 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCompromisedKeyQuarantine

描述：拒絕存取特定動作，如果 IAM 使用者的登入資料遭到洩漏或公開，則由 AWS 團隊套用。請勿移除此政策。相反地，請遵循傳送給您的電子郵件中有關此事件的說明。

AWSCompromisedKeyQuarantine 是 AWS 受管政策。

使用此政策

您可以將 AWSCompromisedKeyQuarantine 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 8 月 11 日 18：04 UTC
- 編輯時間：2020 年 8 月 11 日 18：04 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSCompromisedKeyQuarantineV2

描述：拒絕存取特定動作，如果 IAM 使用者的登入資料遭到洩漏或公開，則由 AWS 團隊套用。請勿移除此政策。相反地，請遵循為您建立的有關此事件的支援案例中指定的說明。

AWSCompromisedKeyQuarantineV2 是 AWS 受管政策。

使用此政策

您可以將 AWSCompromisedKeyQuarantineV2 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 4 月 21 日，UTC 22：30
- 編輯時間：2024 年 10 月 2 日 16：41 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
            "ecs:CreateService",
            "ecs:CreateCluster",
            "ecs:RegisterTaskDefinition",
            "ecr:GetAuthorizationToken",
            "bedrock:CreateModelInvocationJob",
            "bedrock:InvokeModelWithResponseStream",
            "bedrock:CreateFoundationModelAgreement",
            "bedrock:PutFoundationModelEntitlement",
            "bedrock:InvokeModel",
            "s3:CreateBucket",
            "s3:PutBucketCors",
            "s3:GetObject",
            "s3:ListBucket",
            "sagemaker:CreateEndpointConfig",
            "sagemaker:CreateProcessingJob",
            "ses:GetSendQuota",
            "ses:ListIdentities",
            "sts:GetSessionToken",
            "sts:GetFederationToken",
            "amplify:CreateDeployment",
            "amplify:CreateBackendEnvironment",
            "codebuild:CreateProject",
            "glue:CreateJob",
            "iam:DeleteRole",
            "iam:DeleteAccessKey",
            "iam:ListUsers",
```

```
        "lambda:GetEventSourceMapping",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCompromisedKeyQuarantineV3

描述：拒絕存取特定動作， AWS 當 IAM 使用者的登入資料遭到洩露或公開時，由 套用。此政策旨在限制詐騙相關活動可能導致未經授權的費用的潛在損害，同時不會影響現有資源。請勿移除此政策。相反地，請遵循為您建立的有關此事件的支援案例中指定的說明。

AWSCompromisedKeyQuarantineV3 是 AWS 受管政策。

使用此政策

您可以將 AWSCompromisedKeyQuarantineV3 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 8 月 21 日 17：36 UTC
- 編輯時間：2026 年 3 月 16 日 16：27 UTC
- ARN: arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV3

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "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",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:GetEventSourceMapping",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "organizations:LeaveOrganization",
        "organizations:AcceptHandshake",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutEncryptionConfiguration",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
```

```
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel",
        "logs:PutLogEvents",
        "kms:PutKeyPolicy",
        "kms:RetireGrant",
        "kms:RevokeGrant",
        "kms:ScheduleKeyDeletion",
        "kms:DeleteImportedKeyMaterial"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:ViaService" : "true"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSConfigMultiAccountSetupPolicy

描述：允許 Config 呼叫 AWS 服務，並跨組織部署組態資源

`AWSConfigMultiAccountSetupPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 6 月 17 日 18：03 UTC
- 編輯時間：2023 年 2 月 24 日 01：39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSConfigRemediationServiceRolePolicy

描述：允許 AWS Config 代表您修復不合規的資源。

AWSConfigRemediationServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 6 月 18 日 21：21 UTC
- 編輯時間：2019 年 6 月 18 日 21：21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSConfigRoleForOrganizations

描述：允許 AWS Config 呼叫唯讀 AWS Organizations APIs

`AWSConfigRoleForOrganizations` 是 AWS 受管政策。

使用此政策

您可以將 `AWSConfigRoleForOrganizations` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 3 月 19 日，UTC 22：53
- 編輯時間：2020 年 11 月 24 日，UTC 20：19
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSConfigRulesExecutionRole

描述：允許 AWS Lambda 函數存取 AWS Config API 和 AWS Config 定期交付至 Amazon S3 的組態快照。評估自訂 Config 規則組態變更的函數需要此存取權。

`AWSConfigRulesExecutionRole` 是 AWS 受管政策。

使用此政策

您可以將 `AWSConfigRulesExecutionRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 3 月 25 日 17：59 UTC
- 編輯時間：2019 年 5 月 13 日，UTC 21：33
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSConfigServiceRolePolicy

描述：允許 Config 代表您呼叫 AWS 服務和收集資源組態。

AWSConfigServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 5 月 30 日，UTC 23：31
- 編輯時間：2026 年 2 月 24 日 22：57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy

政策版本

政策版本： v90 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "AWSConfigServiceRolePolicyStatementID1",
      "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:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListVpcEndpoints",
```

```
            "app-integrations:GetApplication",
            "app-integrations:GetDataIntegration",
            "app-integrations:GetEventIntegration",
            "app-integrations:ListApplications",
            "app-integrations:ListDataIntegrations",
            "app-integrations:ListEventIntegrationAssociations",
            "app-integrations:ListEventIntegrations",
            "app-integrations:ListTagsForResource",
            "appconfig:GetApplication",
            "appconfig:GetConfigurationProfile",
            "appconfig:GetDeployment",
            "appconfig:GetDeploymentStrategy",
            "appconfig:GetEnvironment",
            "appconfig:GetExtension",
            "appconfig:GetExtensionAssociation",
            "appconfig:GetHostedConfigurationVersion",
            "appconfig:ListApplications",
            "appconfig:ListConfigurationProfiles",
            "appconfig:ListDeployments",
            "appconfig:ListDeploymentStrategies",
            "appconfig:ListEnvironments",
            "appconfig:ListExtensionAssociations",
            "appconfig:ListExtensions",
            "appconfig:ListHostedConfigurationVersions",
            "appconfig:ListTagsForResource",
            "appflow:DescribeConnectorProfiles",
            "appflow:DescribeFlow",
            "appflow:ListFlows",
            "appflow:ListTagsForResource",
            "application-autoscaling:DescribeScalableTargets",
            "application-autoscaling:DescribeScalingPolicies",
            "application-autoscaling:DescribeScheduledActions",
            "application-signals:GetServiceLevelObjective",
            "application-signals:ListServiceLevelObjectiveExclusionWindows",
            "application-signals:ListServiceLevelObjectives",
            "application-signals:ListTagsForResource",
            "applicationinsights:DescribeApplication",
            "applicationinsights:DescribeComponent",
            "applicationinsights:DescribeLogPattern",
            "applicationinsights:ListApplications",
            "applicationinsights:ListComponents",
            "applicationinsights:ListLogPatterns",
            "applicationinsights:ListLogPatternSets",
            "applicationinsights:ListTagsForResource",
```

```
            "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:DescribeObservabilityConfiguration",
            "apprunner:DescribeService",
            "apprunner:DescribeVpcConnector",
            "apprunner:DescribeVpcIngressConnection",
            "apprunner:ListAutoScalingConfigurations",
            "apprunner:ListObservabilityConfigurations",
            "apprunner:ListServices",
            "apprunner:ListTagsForResource",
            "apprunner:ListVpcConnectors",
            "apprunner:ListVpcIngressConnections",
            "appstream:DescribeAppBlockBuilders",
            "appstream:DescribeAppBlocks",
            "appstream:DescribeApplications",
            "appstream:DescribeDirectoryConfigs",
            "appstream:DescribeFleets",
            "appstream:DescribeImageBuilders",
            "appstream:DescribeStacks",
            "appstream:ListTagsForResource",
            "appsync:GetApi",
            "appsync:GetApiAssociation",
            "appsync:GetApiCache",
            "appsync:GetChannelNamespace",
            "appsync:GetDataSource",
            "appsync:GetDomainName",
            "appsync:GetGraphqlApi",
            "appsync:GetSourceApiAssociation",
            "appsync:ListApis",
            "appsync:ListChannelNamespaces",
```

```
            "appsync:ListDataSources",
            "appsync:ListDomainNames",
            "appsync:ListGraphqlApis",
            "appsync:ListSourceApiAssociations",
            "appsync:ListTagsForResource",
            "apptest:GetTestCase",
            "apptest:ListTagsForResource",
            "apptest:ListTestCases",
            "aps:DescribeAlertManagerDefinition",
            "aps:DescribeLoggingConfiguration",
            "aps:DescribeQueryLoggingConfiguration",
            "aps:DescribeRuleGroupsNamespace",
            "aps:DescribeScraper",
            "aps:DescribeScraperLoggingConfiguration",
            "aps:DescribeWorkspace",
            "aps:DescribeWorkspaceConfiguration",
            "aps:ListRuleGroupsNamespaces",
            "aps:ListScrapers",
            "aps:ListTagsForResource",
            "aps:ListWorkspaces",
            "arc-region-switch:GetPlan",
            "arc-region-switch:ListPlans",
            "arc-region-switch:ListRoute53HealthChecks",
            "arc-region-switch:ListTagsForResource",
            "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
            "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",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "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:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeConsumableResource",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:DescribeServiceEnvironments",
        "batch:ListConsumableResources",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-data-exports:GetExport",
```

```
            "bcm-data-exports:ListExports",
            "bcm-data-exports:ListTagsForResource",
            "bedrock-agentcore:GetAgentRuntime",
            "bedrock-agentcore:GetAgentRuntimeEndpoint",
            "bedrock-agentcore:GetBrowser",
            "bedrock-agentcore:GetCodeInterpreter",
            "bedrock-agentcore:GetGateway",
            "bedrock-agentcore:GetGatewayTarget",
            "bedrock-agentcore:GetMemory",
            "bedrock-agentcore:GetWorkloadIdentity",
            "bedrock-agentcore:ListAgentRuntimeEndpoints",
            "bedrock-agentcore:ListAgentRuntimes",
            "bedrock-agentcore:ListBrowsers",
            "bedrock-agentcore:ListCodeInterpreters",
            "bedrock-agentcore:ListGateways",
            "bedrock-agentcore:ListGatewayTargets",
            "bedrock-agentcore:ListMemories",
            "bedrock-agentcore:ListTagsForResource",
            "bedrock-agentcore:ListWorkloadIdentities",
            "bedrock:GetAgent",
            "bedrock:GetAgentActionGroup",
            "bedrock:GetAgentAlias",
            "bedrock:GetAgentCollaborator",
            "bedrock:GetAgentKnowledgeBase",
            "bedrock:GetDataAutomationProject",
            "bedrock:GetDataSource",
            "bedrock:GetFlow",
            "bedrock:GetFlowAlias",
            "bedrock:GetFlowVersion",
            "bedrock:GetGuardrail",
            "bedrock:GetInferenceProfile",
            "bedrock:GetKnowledgeBase",
            "bedrock:GetModelInvocationLoggingConfiguration",
            "bedrock:ListAgentActionGroups",
            "bedrock:ListAgentAliases",
            "bedrock:ListAgentCollaborators",
            "bedrock:ListAgentKnowledgeBases",
            "bedrock:ListAgents",
            "bedrock:ListDataAutomationProjects",
            "bedrock:ListDataSources",
            "bedrock:ListFlowAliases",
            "bedrock:ListFlows",
            "bedrock:ListFlowVersions",
            "bedrock:ListGuardrails",
```

```
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billing:GetBillingView",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing: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:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
```

```
            "cleanrooms:ListTagsForResource",
            "cloud9:DescribeEnvironmentMemberships",
            "cloud9:DescribeEnvironments",
            "cloud9:ListEnvironments",
            "cloud9:ListTagsForResource",
            "cloudformation:BatchDescribeTypeConfigurations",
            "cloudformation:DescribePublisher",
            "cloudformation:DescribeStackInstance",
            "cloudformation:DescribeStacks",
            "cloudformation:DescribeStackSet",
            "cloudformation:DescribeType",
            "cloudformation:GetResource",
            "cloudformation:GetStackPolicy",
            "cloudformation:GetTemplate",
            "cloudformation:ListResources",
            "cloudformation:ListStackInstances",
            "cloudformation:ListStackResources",
            "cloudformation:ListStacks",
            "cloudformation:ListStackSets",
            "cloudformation:ListTypes",
            "cloudfront:DescribeFunction",
            "cloudfront:DescribeKeyValueStore",
            "cloudfront:GetAnycastIpList",
            "cloudfront:GetCachePolicy",
            "cloudfront:GetCloudFrontOriginAccessIdentity",
            "cloudfront:GetConnectionGroup",
            "cloudfront:GetContinuousDeploymentPolicy",
            "cloudfront:GetDistributionTenant",
            "cloudfront:GetFunction",
            "cloudfront:GetKeyGroup",
            "cloudfront:GetMonitoringSubscription",
            "cloudfront:GetOriginAccessControl",
            "cloudfront:GetOriginRequestPolicy",
            "cloudfront:GetPublicKey",
            "cloudfront:GetRealtimeLogConfig",
            "cloudfront:GetResponseHeadersPolicy",
            "cloudfront:GetVpcOrigin",
            "cloudfront:ListAnycastIpLists",
            "cloudfront:ListCachePolicies",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "cloudfront:ListConnectionGroups",
            "cloudfront:ListContinuousDeploymentPolicies",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionTenants",
```

```
        "cloudfront:ListFunctions",
        "cloudfront:ListKeyGroups",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetDashboard",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
```

```
        "codebuild:BatchGetFleets",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListFleets",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections: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:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminGetUser",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeManagedLoginBranding",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeTerms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
```

```
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListTerms",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:ListCampaigns",
        "connect:DescribeAgentStatus",
        "connect:DescribeEmailAddress",
        "connect:DescribeEvaluationForm",
        "connect:DescribeHoursOfOperation",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeUserHierarchyGroup",
        "connect:DescribeView",
        "connect:GetTaskTemplate",
        "connect:ListAgentStatuses",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListEvaluationFormVersions",
```

```
        "connect:ListHoursOfOperationOverrides",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUserHierarchyGroups",
        "connect:ListUsers",
        "connect:ListViews",
        "connect:ListViewVersions",
        "connect:SearchAvailablePhoneNumbers",
        "controltower:GetLandingZone",
        "controltower:ListLandingZones",
        "cur:DescribeReportDefinitions",
        "cur:ListTagsForResource",
        "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",
            "databrew:ListTagsForResource",
            "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",
            "datazone:GetDomain",
            "datazone:GetDomainUnit",
            "datazone:GetEnvironmentAction",
            "datazone:GetEnvironmentBlueprintConfiguration",
            "datazone:GetEnvironmentProfile",
            "datazone:GetGroupProfile",
            "datazone:GetSubscriptionTarget",
            "datazone:GetUserProfile",
            "datazone:ListDomains",
            "datazone:ListDomainUnitsForParent",
            "datazone:ListEntityOwners",
            "datazone:ListEnvironmentActions",
            "datazone:ListEnvironmentBlueprintConfigurations",
            "datazone:ListEnvironmentProfiles",
            "datazone:ListPolicyGrants",
            "datazone:ListProjectMemberships",
            "datazone:ListSubscriptionTargets",
            "datazone:SearchGroupProfiles",
            "datazone:SearchUserProfiles",
            "dax:DescribeClusters",
            "dax:DescribeParameterGroups",
            "dax:DescribeParameters",
            "dax:DescribeSubnetGroups",
            "dax:ListTags",
            "deadline:GetFarm",
            "deadline:GetFleet",
            "deadline:GetLicenseEndpoint",
```

```
            "deadline:GetMonitor",
            "deadline:GetQueue",
            "deadline:GetQueueEnvironment",
            "deadline:GetQueueFleetAssociation",
            "deadline:GetQueueLimitAssociation",
            "deadline:GetStorageProfile",
            "deadline:ListFarms",
            "deadline:ListFleets",
            "deadline:ListLicenseEndpoints",
            "deadline:ListMonitors",
            "deadline:ListQueueEnvironments",
            "deadline:ListQueueFleetAssociations",
            "deadline:ListQueueLimitAssociations",
            "deadline:ListQueues",
            "deadline:ListStorageProfiles",
            "deadline:ListTagsForResource",
            "detective:ListGraphs",
            "detective:ListOrganizationAdminAccount",
            "detective:ListTagsForResource",
            "devicefarm:GetInstanceProfile",
            "devicefarm:GetNetworkProfile",
            "devicefarm:GetProject",
            "devicefarm:GetTestGridProject",
            "devicefarm:ListInstanceProfiles",
            "devicefarm:ListNetworkProfiles",
            "devicefarm:ListProjects",
            "devicefarm:ListTagsForResource",
            "devicefarm:ListTestGridProjects",
            "devops-guru:GetResourceCollection",
            "devops-guru:ListNotificationChannels",
            "directconnect:DescribeConnections",
            "dms:DescribeCertificates",
            "dms:DescribeDataMigrations",
            "dms:DescribeEndpoints",
            "dms:DescribeEventSubscriptions",
            "dms:DescribeReplicationConfigs",
            "dms:DescribeReplicationInstances",
            "dms:DescribeReplicationSubnetGroups",
            "dms:DescribeReplicationTaskAssessmentRuns",
            "dms:DescribeReplicationTasks",
            "dms:ListDataProviders",
            "dms:ListMigrationProjects",
            "dms:ListTagsForResource",
            "docdb-elastic:GetCluster",
```

```
            "docdb-elastic:ListClusters",
            "docdb-elastic:ListTagsForResource",
            "ds:DescribeDirectories",
            "ds:DescribeDomainControllers",
            "ds:DescribeEventTopics",
            "ds:ListLogSubscriptions",
            "ds:ListTagsForResource",
            "dsql:GetCluster",
            "dsql:GetClusterPolicy",
            "dsql:GetVpcEndpointServiceName",
            "dsql:ListClusters",
            "dsql:ListTagsForResource",
            "dynamodb:DescribeContinuousBackups",
            "dynamodb:DescribeGlobalTable",
            "dynamodb:DescribeGlobalTableSettings",
            "dynamodb:DescribeLimits",
            "dynamodb:DescribeTable",
            "dynamodb:DescribeTableReplicaAutoScaling",
            "dynamodb:DescribeTimeToLive",
            "dynamodb:ListTables",
            "dynamodb:ListTagsOfResource",
            "ec2:Describe*",
            "ec2:GetAllowedImagesSettings",
            "ec2:GetEbsEncryptionByDefault",
            "ec2:GetInstanceTypesFromInstanceRequirements",
            "ec2:GetIpamPoolAllocations",
            "ec2:GetIpamPoolCidrs",
            "ec2:GetManagedPrefixListEntries",
            "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
            "ec2:GetNetworkInsightsAccessScopeContent",
            "ec2:GetRouteServerAssociations",
            "ec2:GetRouteServerPropagations",
            "ec2:GetSnapshotBlockPublicAccessState",
            "ec2:GetTransitGatewayRouteTablePropagations",
            "ec2:GetVerifiedAccessEndpointPolicy",
            "ec2:GetVerifiedAccessGroupPolicy",
            "ec2:SearchLocalGatewayRoutes",
            "ec2:SearchTransitGatewayMulticastGroups",
            "ec2:SearchTransitGatewayRoutes",
            "ecr-public:DescribeRepositories",
            "ecr-public:GetRepositoryCatalogData",
            "ecr-public:GetRepositoryPolicy",
            "ecr-public:ListTagsForResource",
            "ecr:BatchGetRepositoryScanningConfiguration",
```

```
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "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:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
```

```
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeListenerAttributes",
        "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:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListVirtualClusters",
```

```
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetIdNamespace",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListIdNamespaces",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "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:GetTargetAccountConfiguration",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "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:GetListElements",
        "frauddetector:GetListsMetadata",
        "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:DescribeContainerFleet",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
```

```
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScalingPolicies",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerFleets",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "gamelift:ValidateMatchmakingRuleSet",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "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:GetDataCatalogEncryptionSettings",
            "glue:GetDevEndpoint",
            "glue:GetDevEndpoints",
            "glue:GetJob",
            "glue:GetJobs",
            "glue:GetMLTransform",
            "glue:GetMLTransforms",
            "glue:GetPartition",
            "glue:GetPartitions",
            "glue:GetRegistry",
            "glue:GetSecurityConfiguration",
            "glue:GetSecurityConfigurations",
            "glue:GetTable",
            "glue:GetTags",
            "glue:GetTrigger",
            "glue:GetWorkflow",
            "glue:ListCrawlers",
            "glue:ListDevEndpoints",
            "glue:ListJobs",
            "glue:ListMLTransforms",
            "glue:ListRegistries",
            "glue:ListTriggers",
            "glue:ListWorkflows",
            "grafana:DescribeWorkspace",
            "grafana:DescribeWorkspaceAuthentication",
            "grafana:DescribeWorkspaceConfiguration",
            "grafana:ListWorkspaces",
            "greengrass:DescribeComponent",
            "greengrass:GetComponent",
            "greengrass:GetDeployment",
            "greengrass:ListComponents",
            "greengrass:ListComponentVersions",
            "greengrass:ListDeployments",
            "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:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatEntitySet",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetTrustedEntitySet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatEntitySets",
        "guardduty:ListThreatIntelSets",
        "guardduty:ListTrustedEntitySets",
        "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:ListPolicies",
            "iam:ListPolicyVersions",
            "iam:ListRolePolicies",
            "iam:ListRoles",
            "iam:ListSAMLProviders",
            "iam:ListServerCertificates",
            "iam:ListUserPolicies",
            "iam:ListUsers",
            "iam:ListVirtualMFADevices",
            "identitystore:DescribeGroup",
            "identitystore:DescribeGroupMembership",
            "identitystore:ListGroupMemberships",
            "identitystore:ListGroupMembershipsForMember",
            "identitystore:ListGroups",
            "imagebuilder:GetComponent",
            "imagebuilder:GetContainerRecipe",
            "imagebuilder:GetDistributionConfiguration",
            "imagebuilder:GetImage",
            "imagebuilder:GetImagePipeline",
            "imagebuilder:GetImageRecipe",
            "imagebuilder:GetInfrastructureConfiguration",
            "imagebuilder:GetLifecyclePolicy",
            "imagebuilder:GetWorkflow",
            "imagebuilder:ListComponentBuildVersions",
            "imagebuilder:ListComponents",
```

```
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "imagebuilder:ListWorkflowBuildVersions",
        "imagebuilder:ListWorkflows",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJob",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetCommand",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:GetV2LoggingOptions",
```

```
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCommands",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackages",
        "iot:ListPackageVersions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID2",
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:ListTagsForResource",
```

```
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetStateTemplate",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListStateTemplates",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
```

```
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "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:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
```

```
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat: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:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra-ranking:ListTagsForResource",
```

```
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "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:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
```

```
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctions",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "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:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
```

```
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetIntegration",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "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:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeSdiSource",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
```

```
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListSdiSources",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "medical-imaging:GetDatastore",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListTagsForResource",
        "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",
        "mpa:GetIdentitySource",
        "mpa:ListIdentitySources",
        "mpa:ListTagsForResource",
        "mq:DescribeBroker",
        "mq:DescribeConfiguration",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "mq:ListTags",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetDirectConnectGatewayAttachment",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
```

```
        "nimble:ListStudios",
        "notifications:GetEventRule",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListNotificationHubs",
        "notifications:ListOrganizationalUnits",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListSinks",
        "oam:ListTagsForResource",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetS3AccessPolicy",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "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:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
```

```
            "organizations:ListRoots",
            "organizations:ListTagsForResource",
            "organizations:ListTargetsForPolicy",
            "osis:GetPipeline",
            "osis:GetResourcePolicy",
            "osis:ListPipelines",
            "osis:ListTagsForResource",
            "panorama:DescribeApplicationInstance",
            "panorama:DescribeApplicationInstanceDetails",
            "panorama:DescribePackage",
            "panorama:DescribePackageVersion",
            "panorama:ListApplicationInstances",
            "panorama:ListNodes",
            "panorama:ListPackages",
            "payment-cryptography:GetAlias",
            "payment-cryptography:GetKey",
            "payment-cryptography:ListAliases",
            "payment-cryptography:ListKeys",
            "payment-cryptography:ListTagsForResource",
            "pca-connector-ad:GetConnector",
            "pca-connector-ad:GetDirectoryRegistration",
            "pca-connector-ad:GetTemplate",
            "pca-connector-ad:GetTemplateGroupAccessControlEntry",
            "pca-connector-ad:ListConnectors",
            "pca-connector-ad:ListDirectoryRegistrations",
            "pca-connector-ad:ListTagsForResource",
            "pca-connector-ad:ListTemplateGroupAccessControlEntries",
            "pca-connector-ad:ListTemplates",
            "pca-connector-scep:GetChallengeMetadata",
            "pca-connector-scep:GetConnector",
            "pca-connector-scep:ListChallengeMetadata",
            "pca-connector-scep:ListConnectors",
            "pca-connector-scep:ListTagsForResource",
            "personalize:DescribeDataset",
            "personalize:DescribeDatasetGroup",
            "personalize:DescribeSchema",
            "personalize:DescribeSolution",
            "personalize:ListDatasetGroups",
            "personalize:ListDatasetImportJobs",
            "personalize:ListDatasets",
            "personalize:ListSchemas",
            "personalize:ListSolutions",
            "personalize:ListTagsForResource",
            "pipes:DescribePipe",
```

```
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeCustomPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListAnalyses",
        "quicksight:ListCustomPermissions",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListFolders",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "quicksight:ListVPCConnections",
        "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:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "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:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeCollection",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListCollections",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "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",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "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",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
```

```
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListOutpostResolvers",
        "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:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
```

```
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "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:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
```

```
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketMetricsConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:ListTableBuckets",
        "s3tables:ListTagsForResource",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:ListVectorBuckets",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListClusters",
```

```
            "sagemaker:ListCodeRepositories",
            "sagemaker:ListDataQualityJobDefinitions",
            "sagemaker:ListDeviceFleets",
            "sagemaker:ListDomains",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListEndpoints",
            "sagemaker:ListFeatureGroups",
            "sagemaker:ListImages",
            "sagemaker:ListImageVersions",
            "sagemaker:ListInferenceComponents",
            "sagemaker:ListInferenceExperiments",
            "sagemaker:ListMlflowTrackingServers",
            "sagemaker:ListModelBiasJobDefinitions",
            "sagemaker:ListModelCards",
            "sagemaker:ListModelCardVersions",
            "sagemaker:ListModelExplainabilityJobDefinitions",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelPackages",
            "sagemaker:ListModelQualityJobDefinitions",
            "sagemaker:ListModels",
            "sagemaker:ListMonitoringSchedules",
            "sagemaker:ListNotebookInstanceLifecycleConfigs",
            "sagemaker:ListNotebookInstances",
            "sagemaker:ListPipelines",
            "sagemaker:ListProcessingJobs",
            "sagemaker:ListProjects",
            "sagemaker:ListSpaces",
            "sagemaker:ListStudioLifecycleConfigs",
            "sagemaker:ListTags",
            "sagemaker:ListUserProfiles",
            "sagemaker:ListWorkteams",
            "scheduler:GetSchedule",
            "scheduler:GetScheduleGroup",
            "scheduler:ListScheduleGroups",
            "scheduler:ListSchedules",
            "scheduler:ListTagsForResource",
            "schemas:DescribeDiscoverer",
            "schemas:DescribeRegistry",
            "schemas:DescribeSchema",
            "schemas:GetResourcePolicy",
            "schemas:ListDiscoverers",
            "schemas:ListRegistries",
            "schemas:ListSchemas",
            "sdb:GetAttributes",
```

```
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetAggregatorV2",
        "securityhub:GetAutomationRuleV2",
        "securityhub:GetConfigurationPolicy",
        "securityhub:GetConfigurationPolicyAssociation",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindingAggregator",
        "securityhub:ListAggregatorsV2",
        "securityhub:ListAutomationRulesV2",
        "securityhub:ListConfigurationPolicies",
        "securityhub:ListConfigurationPolicyAssociations",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:ListFindingAggregators",
        "securityhub:ListTagsForResource",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
```

```
            "ses:DescribeReceiptRuleSet",
            "ses:GetAddonInstance",
            "ses:GetAddonSubscription",
            "ses:GetArchive",
            "ses:GetConfigurationSet",
            "ses:GetConfigurationSetEventDestinations",
            "ses:GetContactList",
            "ses:GetDedicatedIpPool",
            "ses:GetDedicatedIps",
            "ses:GetEmailTemplate",
            "ses:GetIngressPoint",
            "ses:GetRelay",
            "ses:GetRuleSet",
            "ses:GetTemplate",
            "ses:GetTrafficPolicy",
            "ses:ListAddonInstances",
            "ses:ListAddonSubscriptions",
            "ses:ListArchives",
            "ses:ListConfigurationSets",
            "ses:ListContactLists",
            "ses:ListDedicatedIpPools",
            "ses:ListEmailTemplates",
            "ses:ListIngressPoints",
            "ses:ListReceiptFilters",
            "ses:ListReceiptRuleSets",
            "ses:ListRelays",
            "ses:ListRuleSets",
            "ses:ListTagsForResource",
            "ses:ListTemplates",
            "ses:ListTrafficPolicies",
            "shield:DescribeDRTAccess",
            "shield:DescribeProtection",
            "shield:DescribeProtectionGroup",
            "shield:DescribeSubscription",
            "shield:ListProtectionGroups",
            "shield:ListTagsForResource",
            "signer:GetSigningProfile",
            "signer:ListProfilePermissions",
            "signer:ListSigningProfiles",
            "sms-voice:DescribeConfigurationSets",
            "sms-voice:DescribeKeywords",
            "sms-voice:DescribeOptOutLists",
            "sms-voice:DescribePhoneNumbers",
            "sms-voice:DescribePools",
```

```
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeSenderIds",
        "sms-voice:GetProtectConfigurationCountryRuleSet",
        "sms-voice:GetResourcePolicy",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListTagsForResource",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
```

```
            "ssm:ListAssociations",
            "ssm:ListDocuments",
            "ssm:ListResourceDataSync",
            "ssm:ListTagsForResource",
            "sso:DescribeInstanceAccessControlAttributeConfiguration",
            "sso:DescribePermissionSet",
            "sso:GetInlinePolicyForPermissionSet",
            "sso:ListManagedPoliciesInPermissionSet",
            "sso:ListPermissionSets",
            "sso:ListTagsForResource",
            "states:DescribeActivity",
            "states:DescribeStateMachine",
            "states:DescribeStateMachineAlias",
            "states:ListActivities",
            "states:ListStateMachineAliases",
            "states:ListStateMachines",
            "states:ListStateMachineVersions",
            "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",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
```

```
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIpAccessSettings",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetIndexingRules",
        "xray:GetSamplingRules",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "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:*::/account",
        "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:*::/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:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "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/*"
      ]
    }
```

```
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSConfigUserAccess

描述：提供使用 AWS Config 的存取權，包括依資源上的標籤搜尋，以及讀取所有標籤。這不提供設定 Config AWS 的許可，這需要管理權限。

AWSConfigUserAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSConfigUserAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 18 日 19：38 UTC
- 編輯時間：2019 年 3 月 18 日 20：27 UTC
- ARN: arn:aws:iam::aws:policy/AWSConfigUserAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSConnector

描述：啟用對所有 EC2 物件的廣泛讀取/寫入存取、從 'import-to-ec2-' 開始對 S3 儲存貯體的讀取/寫入存取，以及列出所有 S3 儲存貯體的能力，以便 AWS Connector 代表您匯入 VMs。

`AWSConnector` 是 AWS 受管政策。

使用此政策

您可以將 `AWSConnector` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2015 年 2 月 11 日 17：14 UTC
- 編輯時間：2015 年 9 月 28 日 19：50 UTC
- ARN: arn:aws:iam::aws:policy/AWSConnector

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSControlTowerAccountServiceRolePolicy

描述：允許 AWS Control Tower 代您呼叫提供自動化帳戶組態和集中式控管 AWS 的服務。

`AWSControlTowerAccountServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 6 月 5 日 22：04 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        },
        "ForAllValues:StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "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"
    },
    {
      "Sid" : "AllowDeleteConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowPutConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule"
```

```
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowConfigTagResource",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Sid" : "AllowConfigRulesDescribe",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowControlTowerToCreateConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToManageConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
```

```
        "config:DeleteConfigurationAggregator",
        "config:DescribeAggregateComplianceByConfigRules",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/config-aggregator-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToTagConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToPassAggregatorRoleToConfig",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "config.amazonaws.com",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeConfigurationAggregators",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationAggregators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListDelegatedAdministratorsForConfig",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowListDescribeOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
```

```
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSControlTowerCloudTrailRolePolicy

Description： AWS Control Tower 啟用 AWS CloudTrail 做為最佳實務，並將此角色提供給 AWS CloudTrail。 AWS CloudTrail 會擔任此角色來建立和發佈 CloudTrail 日誌

`AWSControlTowerCloudTrailRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSControlTowerCloudTrailRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 11 月 5 日，UTC 21：19
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerCloudTrailRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogStream",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSControlTowerIdentityCenterManagementPolicy

描述：提供在註冊 AWS Control Tower 的成員帳戶中管理 IAM Identity Center (IdC) 資源的許可。只有在客戶在其 AWS Control Tower 登陸區域中選擇加入 IAM IdC 整合時，政策才會連接到 AWSControlTowerAdmin 角色。

`AWSControlTowerIdentityCenterManagementPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSControlTowerIdentityCenterManagementPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 10 月 3 日 18：34 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerIdentityCenterManagementPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowIdentityCenterInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListPermissionSets"
      ],
      "Resource" : "arn:aws:sso:::instance/*"
    },
    {
      "Sid" : "AllowIdentityCenterManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:GetProfile",
        "sso:CreateProfile",
        "sso:UpdateProfile",
        "sso:GetTrust",
```

```
        "sso:CreateTrust",
        "sso:UpdateTrust",
        "sso:CreateApplicationInstance",
        "sso:GetApplicationInstance",
        "sso:GetSSOStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowIdentityCenterDirectoryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:SearchGroups",
        "sso-directory:CreateGroup",
        "sso-directory:SearchUsers",
        "sso-directory:CreateUser",
        "sso-directory:DescribeDirectory"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSControlTowerServiceRolePolicy

描述：提供 AWS Control Tower 管理或使用 AWS 的資源存取權

AWSControlTowerServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSControlTowerServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 5 月 3 日 18：19 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

政策版本

政策版本： v19 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    },
    {
```

```
      "Sid" : "AllowActionsForCloudFormationStackSetOrganizationsTrustedAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ActivateOrganizationsAccess",
        "cloudformation:DescribeOrganizationsAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSCostAndUsageReportAutomationPolicy

描述：授予 許可，以描述帳戶的組織、為 MAP 程式建立 S3 儲存貯體並對其套用標籤、建立成本和用量報告，以及描述成本和用量報告定義。

AWSCostAndUsageReportAutomationPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSCostAndUsageReportAutomationPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 11 月 1 日，UTC 21：27
- 編輯時間：2021 年 11 月 1 日 21：27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataExchangeDataGrantOwnerFullAccess

描述：使用 AWS 管理主控台 和 SDK 授予資料授予擁有者對 AWS 資料交換動作的存取權。

`AWSDataExchangeDataGrantOwnerFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDataExchangeDataGrantOwnerFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 10 月 24 日 14：43 UTC
- 編輯時間：2024 年 10 月 24 日 14：43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantOwnerFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:UpdateDataSet",
        "dataexchange:GetDataSet",
        "dataexchange:DeleteDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:CreateRevision",
        "dataexchange:UpdateRevision",
        "dataexchange:GetRevision",
        "dataexchange:DeleteRevision",
        "dataexchange:RevokeRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:CreateAsset",
        "dataexchange:UpdateAsset",
        "dataexchange:GetAsset",
        "dataexchange:DeleteAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset",
        "dataexchange:CreateDataGrant",
        "dataexchange:GetDataGrant",
        "dataexchange:DeleteDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:PublishToDataGrant",
        "dataexchange:SendDataSetNotification",
        "dataexchange:TagResource",
        "dataexchange:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "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",
            "IMPORT_ASSETS_FROM_LAKE_FORMATION_TAG_POLICY"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataExchangeDataGrantReceiverFullAccess

描述：使用 AWS 管理主控台 和 SDK 讓資料授予接收者存取 AWS 資料交換動作。

`AWSDataExchangeDataGrantReceiverFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDataExchangeDataGrantReceiverFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2024 年 10 月 24 日 14：45 UTC
- 編輯時間：2024 年 10 月 24 日 14：45 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeDataGrantReceiverFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:GetRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:GetAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:GetEventAction",
        "dataexchange:ListEventActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeDataGrantActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:AcceptDataGrant",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:GetReceivedDataGrant"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataExchangeFullAccess

描述：使用 和 SDK 授予 AWS 資料交換 AWS 管理主控台 和 AWS Marketplace 動作的完整存取權。它還提供對充分利用 AWS Data Exchange 所需的相關服務的選取存取權。

AWSDataExchangeFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSDataExchangeFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 11 月 13 日 19：27 UTC
- 編輯時間：2024 年 6 月 24 日 19：54 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeFullAccess

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
```

```
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceProviderActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:DescribeAgreement"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataExchangeProviderFullAccess

描述：使用 和 SDK 授予資料提供者對 AWS 資料交換 AWS 管理主控台 和 AWS Marketplace 動作的存取權。它還提供對充分利用 AWS Data Exchange 所需的相關服務的選取存取權。

`AWSDataExchangeProviderFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDataExchangeProviderFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 11 月 13 日 19：27 UTC
- 編輯時間：2024 年 8 月 15 日 17：32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "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",
        "dataexchange:SendDataSetNotification",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "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"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceActions",
      "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" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDataExchangeReadOnly

描述：使用 和 SDK 授予 AWS 資料交換 AWS 管理主控台 和 AWS Marketplace 動作的唯讀存取權。

AWSDataExchangeReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSDataExchangeReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 11 月 13 日 19：27 UTC
- 編輯時間：2024 年 10 月 24 日 14：40 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataExchangeReadOnly

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetAsset",
        "dataexchange:GetDataSet",
        "dataexchange:GetEventAction",
        "dataexchange:GetJob",
        "dataexchange:GetRevision",
```

```
        "dataexchange:GetDataGrant",
        "dataexchange:GetReceivedDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "dataexchange:ListEventActions",
        "dataexchange:ListJobs",
        "dataexchange:ListRevisionAssets",
        "dataexchange:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceReadOnlyActions",
      "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",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDataExchangeServiceRolePolicyForLicenseManagement

描述：允許 AWS Data Exchange 存取 AWS 服務 和 AWS Data Exchange 用於管理授權的資源。

AWSDataExchangeServiceRolePolicyForLicenseManagement 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 10 月 10 日 14：54 UTC
- 編輯時間：2024 年 10 月 10 日 14：54 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForLicenseManagement

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant"
      ],
```

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

描述：允許 AWS Data Exchange 讀取您 AWS 組織的資料，以判斷 Data Exchange AWS 資料授予授權分發的資格。

`AWSDataExchangeServiceRolePolicyForOrganizationDiscovery` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 10 月 10 日 14：33 UTC
- 編輯時間：2024 年 10 月 10 日 14：33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataExchangeSubscriberFullAccess

描述：使用 和 SDK 授予資料訂閱者對 AWS 資料交換 AWS 管理主控台 和 AWS Marketplace 動作的存取權。它還提供對充分利用 AWS Data Exchange 所需的相關服務的選取存取權。

`AWSDataExchangeSubscriberFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDataExchangeSubscriberFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 11 月 13 日 19：27 UTC

- **編輯時間**：2024 年 5 月 21 日 17：36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
```

```
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataLifecycleManagerServiceRole

描述：為 AWS Data Lifecycle Manager 提供適當的許可，以對 AWS 資源採取動作

`AWSDataLifecycleManagerServiceRole` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDataLifecycleManagerServiceRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 7 月 6 日 19：34 UTC

- **編輯時間**：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "ec2:DescribeAvailabilityZones"
      ],
      "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.*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDataLifecycleManagerServiceRoleForAMIManagement

描述：為 AWS Data Lifecycle Manager 提供適當的許可，以對 AMI Management AWS 的資源採取動作

`AWSDataLifecycleManagerServiceRoleForAMIManagement` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDataLifecycleManagerServiceRoleForAMIManagement` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 10 月 21 日 19：39 UTC
- 編輯時間：2021 年 8 月 19 日 17：03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataLifecycleManagerSSMFullAccess

描述：提供 Amazon Data Lifecycle Manager 許可，以執行在所有 Amazon EC2 執行個體上執行前置和後置指令碼所需的 Systems Manager 動作。

`AWSDataLifecycleManagerSSMFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSDataLifecycleManagerSSMFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 10 月 31 日 20：29 UTC
- 編輯時間：2023 年 11 月 16 日 22：31 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataPipeline_FullAccess

描述：提供資料管道的完整存取權、列出 S3、DynamoDB、Redshift、RDS、SNS 和 IAM 角色的存取權，以及預設角色的 passRole 存取權。

AWSDataPipeline_FullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSDataPipeline_FullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 1 月 19 日 23：14 UTC
- 編輯時間：2017 年 8 月 17 日 18：48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataPipeline_PowerUser

描述：提供資料管道的完整存取權、列出 S3、DynamoDB、Redshift、RDS、SNS 和 IAM 角色的存取權，以及預設角色的 passRole 存取權。

`AWSDataPipeline_PowerUser` 是 AWS 受管政策。

使用此政策

您可以將 AWSDataPipeline_PowerUser 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 1 月 19 日 23：16 UTC
- 編輯時間：2017 年 8 月 17 日 18：49 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataSyncDiscoveryServiceRolePolicy

描述：允許 DataSync Discovery 代表您整合其他 AWS 服務。

`AWSDataSyncDiscoveryServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 3 月 20 日 22：19 UTC
- 編輯時間：2023 年 3 月 20 日 22：19 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataSyncFullAccess

描述：提供 AWS DataSync 的完整存取權，以及對其相依性的最低存取權

AWSDataSyncFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSDataSyncFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 1 月 18 日 19：40 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: arn:aws:iam::aws:policy/AWSDataSyncFullAccess

政策版本

政策版本： v16 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRegions",
        "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",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "DataSyncPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datasync.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataSyncCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/datasync.amazonaws.com/
AWSServiceRoleForDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "datasync.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDataSyncReadOnlyAccess

描述：提供 AWS DataSync 的唯讀存取權

AWSDataSyncReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSDataSyncReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 1 月 18 日 19：18 UTC

- **編輯時間**：2020 年 6 月 30 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDataSyncServiceRolePolicy

描述：允許 DataSync 代表您與其他 AWS 服務整合

AWSDataSyncServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 10 月 9 日 17：45 UTC
- 編輯時間：2025 年 4 月 15 日 16：37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Sid" : "DataSyncCloudWatchLogStreamUpdateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*:log-stream:*"
      ]
    },
    {
      "Sid" : "DataSyncSecretsManagerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSDeadlineCloud-FleetWorker

描述：為 AWS 截止日期的雲端工作者提供在陣列上執行任務的存取權。

AWSDeadlineCloud-FleetWorker 是 AWS 受管政策。

使用此政策

您可以將 AWSDeadlineCloud-FleetWorker 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 4 月 1 日 17：21 UTC
- 編輯時間：2024 年 4 月 1 日 17：21 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunTasksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForWorker",
        "deadline:UpdateWorker",
        "deadline:UpdateWorkerSchedule",
        "deadline:BatchGetJobEntity",
        "deadline:AssumeQueueRoleForWorker"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeadlineCloud-UserAccessFarms

描述：提供使用者工作站對 AWS 截止日期雲端陣列的存取權，具有呼叫其他必要服務的有限唯讀許可。將此政策連接至與您 Studio 相關聯的使用者角色。

`AWSDeadlineCloud-UserAccessFarms` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDeadlineCloud-UserAccessFarms` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 4 月 1 日 16：54 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:CreateBudget",
        "deadline:DeleteBudget",
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue",
        "deadline:GetBudget",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:ListBudgets",
        "deadline:StartSessionsStatisticsAggregation",
        "deadline:UpdateBudget"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarmMembers",
        "deadline:ListFleetMembers",
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
```

```
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetWorker",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
```

```
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeadlineCloud-UserAccessFleets

描述：提供使用者工作站對 AWS 截止日期雲端機群的存取權，具有呼叫其他必要服務的有限唯讀許可。將此政策連接至與您 Studio 相關聯的使用者角色。

`AWSDeadlineCloud-UserAccessFleets` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDeadlineCloud-UserAccessFleets` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 4 月 1 日 17：01 UTC
- 編輯時間：2024 年 4 月 1 日 17：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet",
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
```

```
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleetMembers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:GetFleet",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetWorker",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionsForWorker",
        "deadline:ListWorkers",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER",
```

```
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeadlineCloud-UserAccessJobs

描述：提供使用者工作站對 AWS 期限雲端任務的存取權，具有呼叫其他必要服務的有限唯讀許可。將此政策連接至與您 Studio 相關聯的使用者角色。

`AWSDeadlineCloud-UserAccessJobs` 是 AWS 受管政策。

使用此政策

您可以將 AWSDeadlineCloud-UserAccessJobs 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 4 月 1 日 17：05 UTC
- 編輯時間：2024 年 10 月 7 日 18：24 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
```

```
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListTasks",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDeadlineCloud-UserAccessQueues

描述：提供使用者工作站對 AWS 截止日期雲端佇列的存取權，具有呼叫其他必要服務的有限唯讀許可。將此政策連接至與您 Studio 相關聯的使用者角色。

`AWSDeadlineCloud-UserAccessQueues` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDeadlineCloud-UserAccessQueues` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 4 月 1 日 17：10 UTC
- 編輯時間：2024 年 10 月 7 日 18：25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "ManagerLevelMemberAssociation",
    "Effect" : "Allow",
    "Action" : [
      "deadline:AssociateMemberToJob",
      "deadline:AssociateMemberToQueue"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:QueueMembershipLevels" : [
          "MANAGER"
        ]
      },
      "StringEquals" : {
        "deadline:AssociatedMembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER",
          ""
        ],
        "deadline:MembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER"
        ]
      }
    }
  },
  {
    "Sid" : "ManagerLevelMemberDisassociation",
    "Effect" : "Allow",
    "Action" : [
      "deadline:DisassociateMemberFromJob",
      "deadline:DisassociateMemberFromQueue"
    ],
    "Resource" : [
      "*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeadlineCloud-WorkerHost

描述：為 AWS 截止日期雲端工作者主機提供在陣列中加入機群的存取權。

AWSDeadlineCloud-WorkerHost 是 AWS 受管政策。

使用此政策

您可以將 AWSDeadlineCloud-WorkerHost 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 4 月 1 日 17：28 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "TagWorkerPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:TagResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*/worker/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    },
    {
      "Sid" : "ListFleetTagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListTagsForResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDeepLensLambdaFunctionAccessPolicy

描述：此政策指定 DeepLens 管理 lambda 函數在 DeepLens 裝置上執行所需的許可

AWSDeepLensLambdaFunctionAccessPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSDeepLensLambdaFunctionAccessPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 29 日 15：47 UTC
- 編輯時間：2019 年 6 月 11 日 23：11 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeepLensServiceRolePolicy

描述：Grant AWS DeepLens AWS 服務存取 DeepLens 所需的資源和角色及其相依性，包括 IoT、S3、GreenGrass 和 AWS Lambda。

AWSDeepLensServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSDeepLensServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 11 月 29 日 15：46 UTC
- 編輯時間：2019 年 9 月 25 日 19：25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeepRacerAccountAdminAccess

描述：DeepRacer 管理員存取所有動作，包括在多使用者和單一使用者模式之間切換。

AWSDeepRacerAccountAdminAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSDeepRacerAccountAdminAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 10 月 28 日 01：27 UTC
- 編輯時間：2021 年 10 月 28 日 01：27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDeepRacerCloudFormationAccessPolicy

描述：允許 CloudFormation 代表您建立和管理 AWS 堆疊和資源。

`AWSDeepRacerCloudFormationAccessPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDeepRacerCloudFormationAccessPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 2 月 28 日 21：59 UTC
- 編輯時間：2019 年 6 月 14 日 17：02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeepRacerDefaultMultiUserAccess

描述：DeepRacer MultiUser 預設使用者存取，以在多使用者模式下使用 Deepracer

AWSDeepRacerDefaultMultiUserAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSDeepRacerDefaultMultiUserAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 10 月 28 日 01：27 UTC
- 編輯時間：2021 年 10 月 28 日 01：27 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeepRacerFullAccess

描述：提供 AWS DeepRacer 的完整存取權。也提供相關服務的選取存取權 （例如 S3)。

`AWSDeepRacerFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDeepRacerFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 10 月 5 日，UTC 22：03
- 編輯時間：2020 年 10 月 5 日，22：03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3:::*DeepRacer*/*",
        "arn:aws:s3:::*Deepracer*/*",
        "arn:aws:s3:::*deepracer*/*",
        "arn:aws:s3:::dr-*/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeepRacerRoboMakerAccessPolicy

描述：允許 RoboMaker 代表您建立必要的資源和呼叫 AWS 服務。

AWSDeepRacerRoboMakerAccessPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSDeepRacerRoboMakerAccessPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 2 月 28 日 21：59 UTC
- 編輯時間：2019 年 2 月 28 日，UTC 21：59
- ARN: arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeepRacerServiceRolePolicy

描述：允許 DeepRacer 代表您建立所需的資源和呼叫 AWS 服務。

AWSDeepRacerServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSDeepRacerServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 2 月 28 日 21：58 UTC
- 編輯時間：2019 年 6 月 12 日 20：55 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDenyAll

描述：拒絕所有存取。

AWSDenyAll 是 AWS 受管政策。

使用此政策

您可以將 AWSDenyAll 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 5 月 1 日，UTC 22：36

- **編輯時間**：2023 年 12 月 18 日 16：42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDeviceFarmFullAccess

描述：提供所有 AWS Device Farm 操作的完整存取權。

`AWSDeviceFarmFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSDeviceFarmFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 7 月 13 日 16：37 UTC
- 編輯時間：2015 年 7 月 13 日 16：37 UTC
- ARN: arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeviceFarmServiceRolePolicy

描述：授予 AWS Device Farm 代表您呼叫 EC2 Network APIs許可。

AWSDeviceFarmServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 9 月 20 日、UTC 21：02
- 編輯時間：2022 年 9 月 20 日、UTC 21：02
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDeviceFarmTestGridServiceRolePolicy

描述：授予 AWS Device Farm 代表您呼叫 EC2 APIs許可。

AWSDeviceFarmTestGridServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 5 月 26 日、UTC 22：01
- 編輯時間：2021 年 5 月 26 日，UTC 22：01
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDirectConnectFullAccess

描述：透過 提供 AWS Direct Connect 的完整存取權 AWS 管理主控台。

`AWSDirectConnectFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSDirectConnectFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2019 年 4 月 30 日 15：29 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDirectConnectReadOnlyAccess

描述：透過 提供 AWS Direct Connect 的唯讀存取權 AWS 管理主控台。

AWSDirectConnectReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSDirectConnectReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2020 年 5 月 18 日 18：48 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDirectConnectServiceRolePolicy

描述：提供 AWS Direct Connect 許可，以代表您建立和管理 AWS 資源。

`AWSDirectConnectServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 1 月 14 日 18：35 UTC
- 編輯時間：2021 年 1 月 14 日 18：35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDirectoryServiceDataFullAccess

描述：提供 AWS Directory Service Data 的完整存取權。

`AWSDirectoryServiceDataFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDirectoryServiceDataFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- **建立時間**：2024 年 9 月 18 日 21：45 UTC
- **編輯時間**：2024 年 9 月 18 日 21：45 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:AddGroupMember",
        "ds-data:CreateGroup",
        "ds-data:CreateUser",
        "ds-data:DeleteGroup",
        "ds-data:DeleteUser",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:DisableUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:RemoveGroupMember",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers",
        "ds-data:UpdateGroup",
        "ds-data:UpdateUser"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDirectoryServiceDataReadOnlyAccess

描述：提供 AWS Directory Service Data 的唯讀存取權

`AWSDirectoryServiceDataReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDirectoryServiceDataReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 9 月 18 日 22：00 UTC
- 編輯時間：2024 年 9 月 18 日 22：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDirectoryServiceFullAccess

描述：提供 AWS Directory Service 的完整存取權。

`AWSDirectoryServiceFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDirectoryServiceFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2024 年 4 月 2 日 20：38 UTC
- ARN: arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectoryServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "iam:ListRoles",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DirectoryServiceEventTopic",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
    },
    {
      "Sid" : "DirectoryServiceOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DirectoryServiceTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSDirectoryServiceReadOnlyAccess

描述：提供 AWS Directory Service 的唯讀存取權。

`AWSDirectoryServiceReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSDirectoryServiceReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2018 年 9 月 25 日，UTC 21：54
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDirectoryServiceServiceRolePolicy

描述： Directory Service 連結角色的政策

AWSDirectoryServiceServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 7 月 11 日 00：22 UTC
- 編輯時間：2025 年 7 月 11 日 00：22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSDirectoryServiceServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
```

```
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSDiscoveryContinuousExportFirehosePolicy

描述：提供 AWS Discovery Continuous Export 所需 AWS 資源的寫入存取權

AWSDiscoveryContinuousExportFirehosePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSDiscoveryContinuousExportFirehosePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 8 月 9 日 18：29 UTC
- 編輯時間：2021 年 6 月 8 日 17：32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSDMSFleetAdvisorServiceRolePolicy

描述：允許 DMS Fleet Advisor 代表您管理 CloudWatch 指標。

`AWSDMSFleetAdvisorServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 3 月 6 日 09：10 UTC
- 編輯時間：2023 年 3 月 6 日 09：10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSDMSServerlessServiceRolePolicy

描述：授予 AWS DMS Serverless 許可，以代表您在帳戶中建立和管理 DMS 資源

AWSDMSServerlessServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 5 月 18 日 20：28 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:ModifyReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:ModifyReplicationInstance",
        "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:*"
      ]
    },
    {
      "Sid" : "id4",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObjectTagging"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id6",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSEC2CapacityManagerServiceRolePolicy

描述：允許 EC2 Capacity Manager 代表您管理容量資源並與 AWS Organizations 整合。

`AWSEC2CapacityManagerServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 10 月 9 日，UTC 22：04
- 編輯時間：2025 年 10 月 9 日 22：04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityManagerServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsDefaultReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsListDelegatedAdministratorsAction",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "ec2.capacitymanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSEC2CapacityReservationFleetRolePolicy

描述：允許 EC2 CapacityReservation Fleet 服務管理容量保留

AWSEC2CapacityReservationFleetRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 9 月 29 日 14：43 UTC
- 編輯時間：2025 年 3 月 3 日 23：22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "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"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSEC2FleetServiceRolePolicy

描述：允許 EC2 機群啟動和管理執行個體。

AWSEC2FleetServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 3 月 21 日 00：08 UTC
- 編輯時間：2020 年 5 月 4 日，20：10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSEC2SpotFleetServiceRolePolicy

描述：允許 EC2 Spot Fleet 啟動和管理 Spot 機群執行個體

AWSEC2SpotFleetServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 23 日 19：13 UTC
- 編輯時間：2020 年 3 月 16 日 19：16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSEC2SpotServiceRolePolicy

描述：允許 EC2 Spot 啟動和管理 Spot 執行個體

AWSEC2SpotServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 9 月 18 日 18：51 UTC
- 編輯時間：2018 年 12 月 12 日 00：13 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSEC2SqlHaInstancePolicy

描述：Amazon EC2 執行個體許可，允許 EC2 SQL 高可用性服務透過 EC2 執行個體描述檔偵測執行個體高可用性狀態。

AWSEC2SqlHaInstancePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSEC2SqlHaInstancePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 13 日 01：49 UTC

- **編輯時間**：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2SqlHaInstancePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSEc2SqlHa" : "*"
        }
      }
    },
    {
      "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSEC2SqlHaServiceRolePolicy

描述：偵測待命/被動執行個體的 EC2 SQL 高可用性服務許可

AWSEC2SqlHaServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 11 月 13 日 01：34 UTC
- 編輯時間：2025 年 11 月 13 日 01：34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SqlHaServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMSendCommandToTaggedInstances",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendCommandOfOwnedDoc",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-DetectSqlHa*"
      ]
```

```
    },
    {
      "Sid" : "AllowSSMNonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2NonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventsMutateManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2sqlha.amazonaws.com",
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    },
    {
      "Sid" : "AllowEventsNonMutatingManagedRule",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSEC2VssSnapshotPolicy

描述：此政策會連接至連接至 Amazon EC2 Windows 執行個體的 IAM 角色，讓 Amazon EC2 VSS 解決方案能夠建立標籤並將其新增至 Amazon Machine Image (AMI) 和 EBS 快照。

`AWSEC2VssSnapshotPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSEC2VssSnapshotPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 3 月 27 日 16：32 UTC
- 編輯時間：2024 年 11 月 20 日 17：44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceInfo",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "CreateImageWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateImageAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
```

```
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateImage",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsAfterResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppConsistent",
            "Device"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeImagesAndSnapshots",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSECRPullThroughCache_ServiceRolePolicy

描述：允許存取由 AWS ECR 提取快取使用或管理 AWS 的服務和資源

AWSECRPullThroughCache_ServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 26 日 21：51 UTC
- 編輯時間：2025 年 3 月 6 日 21：22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage",
        "ecr:BatchGetImage",
        "ecr:BatchImportUpstreamImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetImageCopyStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkCustomPlatformforEC2Role

描述：在您的自訂平台建置器環境中提供執行個體，以啟動 EC2 執行個體、建立 EBS 快照和 AMI、將日誌串流至 Amazon CloudWatch Logs，以及將成品存放在 Amazon S3 中。

`AWSElasticBeanstalkCustomPlatformforEC2Role` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticBeanstalkCustomPlatformforEC2Role` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 2 月 21 日 22：50 UTC
- 編輯時間：2017 年 2 月 21 日 22：50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkEnhancedHealth

描述：運作狀態監控系統的 AWS 彈性 Beanstalk 服務政策

AWSElasticBeanstalkEnhancedHealth 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticBeanstalkEnhancedHealth 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策

- **建立時間**：2016 年 2 月 8 日 23：17 UTC
- **編輯時間**：2018 年 4 月 9 日，UTC 22：12
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticBeanstalkMaintenance

描述： AWS Elastic Beanstalk 服務角色政策，授予有限的許可，以代表您更新 資源以進行維護。

`AWSElasticBeanstalkMaintenance` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 1 月 11 日 23：22 UTC
- 編輯時間：2024 年 4 月 29 日，UTC 21：48
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

描述：此政策適用於 AWS Elastic Beanstalk 服務角色，用於執行 Elastic Beanstalk 環境的受管更新。此政策不應連接到其他使用者或角色。此政策授予廣泛的許可，以跨許多 AWS 服務建立和管理資源，包括 AutoScaling、EC2、ECS、Elastic Load Balancing 和 CloudFormation。此政策也允許傳遞可與這些服務搭配使用的任何 IAM 角色。

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 3 月 3 日 22：18 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances",
            "AllocateAddress"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

描述： AWS Elastic Beanstalk 服務角色政策，授予受管更新的有限許可。

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 21 日，UTC 22：35
- 編輯時間：2026 年 3 月 13 日 16：12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
```

```
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElasticBeanstalkAPIs",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
```

```
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
```

```
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
```

```
    },
    {
      "Sid" : "EC2LaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*"
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances",
            "AllocateAddress"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkMulticontainerDocker

描述：提供多容器 Docker 環境中的執行個體存取權，以使用 Amazon EC2 Container Service 管理容器部署任務。

`AWSElasticBeanstalkMulticontainerDocker` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticBeanstalkMulticontainerDocker` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 2 月 8 日 23：15 UTC
- 編輯時間：2026 年 3 月 12 日 14：12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
          ]
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
```

```
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : "arn:aws:bedrock:*::foundation-model/anthropic.claude-*"
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkReadOnly

描述：授予唯讀許可。明確允許運算子直接存取，以擷取與 AWS Elastic Beanstalk 應用程式相關的資源資訊。

AWSElasticBeanstalkReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticBeanstalkReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 1 月 22 日 19：02 UTC
- 編輯時間：2021 年 1 月 22 日 19：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticBeanstalkRoleCore

描述：AWSElasticBeanstalkRoleCore (Elastic Beanstalk 操作角色） 允許 Web 服務環境的核心操作。

`AWSElasticBeanstalkRoleCore` 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticBeanstalkRoleCore 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 6 月 5 日 21：48 UTC
- 編輯時間：2024 年 4 月 30 日 00：01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:ReleaseAddress",
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:DeleteLaunchTemplate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:*Tags"
      ],
```

```
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*/*",
        "arn:aws:s3:::elasticbeanstalk-env-resources-*/*"
      ]
```

```
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CancelUpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Create*",
        "elasticloadbalancing:Delete*",
        "elasticloadbalancing:Modify*",
        "elasticloadbalancing:RegisterTargets",
```

```
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*"
      ]
    },
    {
      "Sid" : "ListAPIs",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "logs:Describe*",
        "ec2:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "elasticloadbalancing:Describe*",
        "rds:Describe*",
        "sns:List*",
        "iam:List*",
        "acm:Describe*",
        "acm:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkRoleCWL

描述：(Elastic Beanstalk 操作角色） 允許環境管理 Amazon CloudWatch Logs 日誌群組。

AWSElasticBeanstalkRoleCWL 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticBeanstalkRoleCWL 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 6 月 5 日，UTC 21：49
- 編輯時間：2020 年 6 月 5 日，UTC 21：49
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL

政策版本

政策版本： v1 （ 預設 ）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticBeanstalkRoleECS

描述：(Elastic Beanstalk 操作角色） 允許多容器 Docker 環境管理 Amazon ECS 叢集。

AWSElasticBeanstalkRoleECS 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticBeanstalkRoleECS 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 6 月 5 日，UTC 21：47
- 編輯時間：2023 年 3 月 23 日 22：43 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkRoleRDS

描述：(Elastic Beanstalk 操作角色） 允許環境整合 Amazon RDS 執行個體。

AWSElasticBeanstalkRoleRDS 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticBeanstalkRoleRDS 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 6 月 5 日 21：46 UTC
- 編輯時間：2020 年 6 月 5 日 21：46 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkRoleSNS

描述：(Elastic Beanstalk 操作角色） 允許環境啟用 Amazon SNS 主題整合。

AWSElasticBeanstalkRoleSNS 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticBeanstalkRoleSNS 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 6 月 5 日 21：46 UTC
- 編輯時間：2020 年 6 月 5 日 21：46 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticBeanstalkRoleWorkerTier

描述：(Elastic Beanstalk 操作角色） 允許工作者環境層建立 Amazon DynamoDB 資料表和 Amazon SQS 佇列。

`AWSElasticBeanstalkRoleWorkerTier` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticBeanstalkRoleWorkerTier` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 6 月 5 日，UTC 21：43

- **編輯時間**：2020 年 6 月 5 日 21：43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticBeanstalkService

描述：此政策位於棄用路徑上。如需指引，請參閱 文件：https：//https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html. AWS Elastic Beanstalk Service 角色政策，該政策授予代表您建立和管理資源（即 AutoScaling、EC2, S3、CloudFormation、ELB 等）的許可。

`AWSElasticBeanstalkService` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticBeanstalkService` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 4 月 11 日 20：27 UTC
- 編輯時間：2023 年 5 月 10 日 19：29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

政策版本

政策版本： v17（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkServiceRolePolicy

描述： AWS Elastic Beanstalk 服務連結角色政策，授予代表您建立和管理資源（即 AutoScaling、EC2, S3、CloudFormation、ELB 等）的許可。

`AWSElasticBeanstalkServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 9 月 13 日 23：46 UTC
- 編輯時間：2019 年 6 月 6 日 21：59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

政策版本

政策版本： v6（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkWebTier

描述：提供 Web 伺服器環境中的執行個體存取權，以將日誌檔案上傳至 Amazon S3。

`AWSElasticBeanstalkWebTier` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticBeanstalkWebTier` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 2 月 8 日 23：08 UTC
- 編輯時間：2026 年 3 月 12 日 14：27 UTC

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

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : "arn:aws:bedrock:*::foundation-model/anthropic.claude-*"
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticBeanstalkWorkerTier

描述：提供工作者環境中的執行個體存取權，以將日誌檔案上傳到 Amazon S3、使用 Amazon SQS 監控應用程式的任務佇列、使用 Amazon DynamoDB 執行領導者選擇，以及向 Amazon CloudWatch 發佈用於運作狀態監控的指標。

`AWSElasticBeanstalkWorkerTier` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticBeanstalkWorkerTier` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2016 年 2 月 8 日 23：12 UTC
- 編輯時間：2026 年 3 月 12 日 14：27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*"
      ]
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : "arn:aws:bedrock:*::foundation-model/anthropic.claude-*"
    },
    {
      "Sid" : "AIEnvironmentAnalysisInvokeInferenceProfile",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : "arn:aws:bedrock:*:*:inference-profile/*anthropic.claude-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AIEnvironmentAnalysisReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels",
        "elasticbeanstalk:DescribeEvents",
        "elasticbeanstalk:DescribeEnvironmentHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticDisasterRecoveryAgentInstallationPolicy

描述：此政策允許安裝 AWS 複寫代理程式，此代理程式與 AWS Elastic Disaster Recovery (DRS) 搭配使用，以復原外部伺服器 AWS。將此政策連接到您在 複寫代理程式安裝步驟期間提供的憑證的 IAM AWS 使用者或角色。

`AWSElasticDisasterRecoveryAgentInstallationPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryAgentInstallationPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 17 日 10：37 UTC
- 編輯時間：2023 年 11 月 27 日 12：38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticDisasterRecoveryAgentPolicy

描述：此政策允許使用 AWS 複寫代理程式，此代理程式與 AWS Elastic Disaster Recovery (DRS) 搭配使用，以復原來源伺服器 AWS。我們不建議您將此政策連接至 IAM 使用者或角色。

`AWSElasticDisasterRecoveryAgentPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryAgentPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 11 月 17 日 10：32 UTC
- 編輯時間：2023 年 11 月 27 日 13：44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticDisasterRecoveryConsoleFullAccess

描述：此政策提供 AWS Elastic Disaster Recovery (DRS) 所有公有 APIs 的完整存取權，以及讀取 KMS 金鑰、 License Manager、Resource Groups、Elastic Load Balancing、IAM 和 EC2 資訊的許可。將此政策連接至您的 IAM 使用者或角色。

`AWSElasticDisasterRecoveryConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 17 日 10：46 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticDisasterRecoveryConsoleFullAccess_v2

描述：此政策提供 AWS 對 Elastic Disaster Recovery (AWS DRS) 的所有公有 APIs 的完整存取權，以及 AWS DRS 主控台使用之 AWS 其他服務中的所有公APIs。將此政策連接至您的使用者或角色。

AWSElasticDisasterRecoveryConsoleFullAccess_v2 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticDisasterRecoveryConsoleFullAccess_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 11 月 27 日 13：35 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
```

```
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
```

```
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "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"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess38",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess39",
      "Effect" : "Allow",
      "Action" : "ec2:CreateFleet",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess40",
      "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" : [
            "CreateFleet"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess41",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess42",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess43",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ConsoleFullAccess44",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticDisasterRecoveryConversionServerPolicy

描述：此政策會連接至 AWS Elastic Disaster Recovery Conversion 伺服器的執行個體角色。此政策允許 Elastic Disaster Recovery (DRS) 轉換伺服器，這是 Elastic Disaster Recovery 啟動的 EC2 執行個體，可與 DRS 服務通訊。具有此政策的 IAM 角色由 DRS 連接至 DRS 轉換伺服器（做為 EC2 執行個體設定檔），該伺服器會視需要由 DRS 自動啟動和終止。我們不建議您將此政策連接至 IAM 使用者或角色。當使用者選擇使用 DRS 主控台、CLI 或 API 復原來源伺服器時，Elastic Disaster Recovery 會使用 DRS Conversion Server。

`AWSElasticDisasterRecoveryConversionServerPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryConversionServerPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 11 月 17 日 13：42 UTC
- 編輯時間：2023 年 11 月 27 日 13：13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

描述：此政策允許 AWS Elastic Disaster Recovery (DRS) 支援跨帳戶複寫和跨帳戶容錯回復。

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 5 月 14 日 07：16 UTC
- 編輯時間：2024 年 1 月 17 日 13：19 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticDisasterRecoveryEc2InstancePolicy

描述：此政策允許安裝和使用 AWS 複寫代理程式， AWS Elastic Disaster Recovery (DRS) 會使用此代理程式來復原在 EC2 上執行的來源伺服器（跨區域或跨可用區）。具有此政策的 IAM 角色應附加（做為 EC2 執行個體描述檔）至 EC2 執行個體。

`AWSElasticDisasterRecoveryEc2InstancePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryEc2InstancePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 5 月 26 日 12：30 UTC

- **編輯時間**：2023 年 11 月 27 日 13：39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticDisasterRecoveryFailbackInstallationPolicy

描述：您可以將 AWSElasticDisasterRecoveryFailbackInstallationPolicy 政策連接至 IAM 身分。此政策允許安裝 Elastic Disaster Recovery 容錯回復用戶端，此用戶端用於將復原執行個體容錯回復至原始來源基礎設施。將此政策連接到您在執行 Elastic Disaster Recovery 容錯回復用戶端時提供憑證的 IAM 使用者或角色。

`AWSElasticDisasterRecoveryFailbackInstallationPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryFailbackInstallationPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 17 日 11：02 UTC
- 編輯時間：2023 年 11 月 27 日 13：43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticDisasterRecoveryFailbackPolicy

描述：此政策允許使用 Elastic Disaster Recovery 容錯回復用戶端，此用戶端用於將復原執行個體容錯回復至原始來源基礎設施。我們不建議您將此政策連接至 IAM 使用者或角色。

AWSElasticDisasterRecoveryFailbackPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticDisasterRecoveryFailbackPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 11 月 17 日 10：41 UTC
- 編輯時間：2023 年 11 月 27 日 12：56 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticDisasterRecoveryLaunchActionsPolicy

描述：此政策可讓您使用 Amazon SSM 和其他服務所需的許可，在 AWS Elastic Disaster Recovery (AWS DRS) 中執行啟動後動作。將此政策連接至您的 IAM 角色或使用者。

`AWSElasticDisasterRecoveryLaunchActionsPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryLaunchActionsPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 9 月 13 日 07：38 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "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/AWSDistroOTel-*",
        "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/AWSDistroOTel-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
        "arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
        "arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
        "arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
        "arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
        "arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
        "arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
        "arn:aws:ssm:*::automation-definition/AWSResilienceHub-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAPTools-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSQLServer-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSSO-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSupport-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSystemsManagerSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatch-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatchAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonECS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEFSUtils-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEKS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector2-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInternal-*:*",
        "arn:aws:ssm:*::automation-definition/AwsEnaNetworkDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AwsVssComponents-*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticDisasterRecoveryNetworkReplicationPolicy

描述：此政策允許 AWS Elastic Disaster Recovery (DRS) 支援網路複寫。

AWSElasticDisasterRecoveryNetworkReplicationPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticDisasterRecoveryNetworkReplicationPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 6 月 11 日 12：36 UTC
- 編輯時間：2024 年 1 月 2 日 13：25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticDisasterRecoveryReadOnlyAccess

描述：您可以將 AWSElasticDisasterRecoveryReadOnlyAccess 政策連接至 IAM 身分。此政策提供 Elastic Disaster Recovery (DRS) 所有唯讀公有 APIs 的許可，以及 DRS 主控台完整唯讀使用所需 AWS 其他服務的一些唯讀 APIs。將此政策連接至您的 IAM 使用者或角色。

`AWSElasticDisasterRecoveryReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2021 年 11 月 17 日 10：50 UTC
- **編輯時間**：2024 年 7 月 29 日 19：39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticDisasterRecoveryRecoveryInstancePolicy

描述：此政策會連接到 Elastic Disaster Recovery 復原執行個體的執行個體角色。此政策允許 Elastic Disaster Recovery (DRS) Recovery 執行個體，這是 Elastic Disaster Recovery 啟動的 EC2 執行個體 - 與 DRS 服務通訊，並能夠容錯回復至其原始來源基礎設施。Elastic Disaster Recovery 會將具有此政策的 IAM 角色（做為 EC2 執行個體設定檔）連接至 DRS 復原執行個體。我們不建議您將此政策連接至 IAM 使用者或角色。

`AWSElasticDisasterRecoveryRecoveryInstancePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryRecoveryInstancePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 11 月 17 日 10：20 UTC
- 編輯時間：2023 年 11 月 27 日 13：11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:UpdateReplicationCertificateForDrs",
        "drs:NotifyReplicationServerAuthenticationForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
```

```
      "Sid" : "DRSRecoveryInstancePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticDisasterRecoveryReplicationServerPolicy

描述：此政策會連接到 Elastic Disaster Recovery Replication 伺服器的執行個體角色。此政策允許 Elastic Disaster Recovery (DRS) 複寫伺服器，這是 Elastic Disaster Recovery 啟動的 EC2 執行個體 - 與 DRS 服務通訊，並在您的 中建立 EBS 快照 AWS 帳戶。Elastic Disaster Recovery 會將具有此政策的 IAM 角色（做為 EC2 執行個體描述檔）連接至 DRS 複寫伺服器，並視需要由 DRS 自動啟動和終止。DRS 複寫伺服器用於促進從外部伺服器到 的資料複寫 AWS，作為 DRS 管理的復原程序的一部分。我們不建議您將此政策連接至 IAM 使用者或角色。

`AWSElasticDisasterRecoveryReplicationServerPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElasticDisasterRecoveryReplicationServerPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 11 月 17 日 13：34 UTC
- 編輯時間：2023 年 11 月 27 日 13：28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

政策版本

政策版本： v3（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticDisasterRecoveryServiceRolePolicy

描述：此政策允許 Elastic Disaster Recovery 代表您管理 AWS 資源。

`AWSElasticDisasterRecoveryServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 17 日 10：56 UTC
- 編輯時間：2025 年 1 月 5 日 14：07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "ec2:DescribeNetworkInterfaces"
      ],
      "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/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "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" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy29",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy31",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy32",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy33",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticDisasterRecoveryStagingAccountPolicy

描述：此政策允許唯讀存取 AWS Elastic Disaster Recovery (DRS) 資源，例如來源伺服器和任務。它也允許建立轉換後的快照，並與特定帳戶共用該 EBS 快照。

AWSElasticDisasterRecoveryStagingAccountPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticDisasterRecoveryStagingAccountPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 5 月 26 日 09：49 UTC
- 編輯時間：2023 年 11 月 27 日 13：07 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

描述： AWS Elastic Disaster Recovery (DRS) 使用此政策將來源伺服器復原至個別的目標帳戶，並允許容錯回復。我們不建議您將此政策連接至 IAM 使用者或角色。

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 是 AWS 受管政策。

使用此政策

您可以將 AWSElasticDisasterRecoveryStagingAccountPolicy_v2 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 1 月 5 日 12：11 UTC
- 編輯時間：2023 年 11 月 27 日 13：32 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElasticLoadBalancingClassicServiceRolePolicy

描述： AWS Elastic Load Balancing 控制平面的服務連結角色政策 - Classic

`AWSElasticLoadBalancingClassicServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 9 月 19 日，UTC 22：36
- 編輯時間：2019 年 10 月 7 日 23：04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSElasticLoadBalancingServiceRolePolicy

描述： AWS Elastic Load Balancing 控制平面的服務連結角色政策

AWSElasticLoadBalancingServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 9 月 19 日，UTC 22：19
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:ReleaseAddress",
        "ec2:UnassignIpv6Addresses",
        "ec2:DescribeVpcPeeringConnections",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:AllocateIpamPoolCidr",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSElementalMediaConnectCreateBridge

描述：提供建立 MediaConnect Gateway Bridges 及其所有相關聯子資源的完整存取權。

`AWSElementalMediaConnectCreateBridge` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaConnectCreateBridge` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2026 年 3 月 19 日 16：57 UTC
- 編輯時間：2026 年 3 月 19 日 16：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateBridge`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:CreateBridge",
        "mediaconnect:AddBridgeSources",
        "mediaconnect:AddBridgeOutputs"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:bridge:*:*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeSource/*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeOutput/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaConnectCreateFlow

描述：提供建立 MediaConnect Flows 及其所有相關聯子資源的完整存取權。

`AWSElementalMediaConnectCreateFlow` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaConnectCreateFlow` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2026 年 3 月 19 日 16：57 UTC
- 編輯時間：2026 年 3 月 19 日 16：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectCreateFlow`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "mediaconnect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:CreateFlow",
        "mediaconnect:AddFlowSources",
        "mediaconnect:AddFlowOutputs",
        "mediaconnect:GrantFlowEntitlements",
        "mediaconnect:AddFlowMediaStreams",
        "mediaconnect:AddFlowVpcInterfaces",
        "mediaconnect:TagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:mediaconnect:*:*:flow:*:*",
        "arn:aws:mediaconnect:*:*:source:*:*",
        "arn:aws:mediaconnect:*:*:output:*:*",
        "arn:aws:mediaconnect:*:*:entitlement:*:*",
        "arn:aws:mediaconnect:*:*:flow:*:*/vpcInterface/*",
        "arn:aws:mediaconnect:*:*:flow:*:*/mediaStream/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaConnectDeleteBridge

描述：提供刪除 MediaConnect Gateway Bridges 及其所有相關聯子資源的完整存取權。

`AWSElementalMediaConnectDeleteBridge` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaConnectDeleteBridge` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2026 年 3 月 19 日 19：57 UTC
- 編輯時間：2026 年 3 月 19 日 19：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteBridge`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DeleteBridge",
        "mediaconnect:RemoveBridgeSource",
        "mediaconnect:RemoveBridgeOutput"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:bridge:*:*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeSource/*",
        "arn:aws:mediaconnect:*:*:bridge:*:*/bridgeOutput/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElementalMediaConnectDeleteFlow

描述：提供刪除 MediaConnect Flows 及其所有相關聯子資源的完整存取權。

`AWSElementalMediaConnectDeleteFlow` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaConnectDeleteFlow` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2026 年 3 月 19 日 19：57 UTC
- 編輯時間：2026 年 3 月 19 日 19：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConnectDeleteFlow

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DeleteFlow",
        "mediaconnect:RemoveFlowSource",
        "mediaconnect:RemoveFlowOutput",
        "mediaconnect:RevokeFlowEntitlement",
        "mediaconnect:RemoveFlowMediaStream",
        "mediaconnect:RemoveFlowVpcInterface"
      ],
      "Resource" : [
        "arn:aws:mediaconnect:*:*:flow:*:*",
        "arn:aws:mediaconnect:*:*:source:*:*",
        "arn:aws:mediaconnect:*:*:output:*:*",
        "arn:aws:mediaconnect:*:*:entitlement:*:*",
        "arn:aws:mediaconnect:*:*:flow:*:*/vpcInterface/*",
        "arn:aws:mediaconnect:*:*:flow:*:*/mediaStream/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaConnectFullAccess

描述：提供 AWS Elemental MediaConnect 資源的完整存取權。

`AWSElementalMediaConnectFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaConnectFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 2 月 12 日 20：07 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaConnectReadOnlyAccess

描述：提供 AWS Elemental MediaConnect 資源的唯讀存取權。

`AWSElementalMediaConnectReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaConnectReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 2 月 12 日 20：07 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:ListBridges",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaConvertFullAccess

描述：透過 AWS 管理主控台 和 SDK 提供 AWS Elemental MediaConvert 的完整存取權。

AWSElementalMediaConvertFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSElementalMediaConvertFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 6 月 25 日 19：25 UTC
- 編輯時間：2019 年 6 月 10 日 22：52 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElementalMediaConvertReadOnly

描述：透過 AWS 管理主控台 和 SDK 提供 AWS Elemental MediaConvert 的唯讀存取權。

`AWSElementalMediaConvertReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaConvertReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 6 月 25 日 19：25 UTC
- 編輯時間：2019 年 6 月 10 日 22：52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaLiveFullAccess

描述：提供 AWS Elemental MediaLive 資源的完整存取權

`AWSElementalMediaLiveFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaLiveFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 7 月 8 日 17：07 UTC
- 編輯時間：2020 年 7 月 8 日 17：07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaLiveReadOnly

描述：提供 AWS Elemental MediaLive 資源的唯讀存取權

`AWSElementalMediaLiveReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 AWSElementalMediaLiveReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 7 月 8 日 16：38 UTC
- 編輯時間：2024 年 7 月 22 日 17：08 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaPackageFullAccess

描述：提供 AWS Elemental MediaPackage 資源的完整存取權

AWSElementalMediaPackageFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSElementalMediaPackageFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 12 月 29 日，UTC 23：39
- 編輯時間：2017 年 12 月 29 日，UTC 23：39
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaPackageReadOnly

描述：提供 AWS Elemental MediaPackage 資源的唯讀存取權

`AWSElementalMediaPackageReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaPackageReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 12 月 30 日 00：04 UTC
- 編輯時間：2017 年 12 月 30 日 00：04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackage:List*",
      "mediapackage:Describe*"
    ],
    "Resource" : "*"
  }
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaPackageV2FullAccess

描述：提供 AWS Elemental MediaPackageV2 資源的完整存取權。

`AWSElementalMediaPackageV2FullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaPackageV2FullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 7 月 25 日，UTC 20：29
- 編輯時間：2023 年 7 月 25 日 20：29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSElementalMediaPackageV2ReadOnly

描述：提供 AWS Elemental MediaPackageV2 資源的唯讀存取權。

`AWSElementalMediaPackageV2ReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaPackageV2ReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 7 月 25 日 20：31 UTC
- 編輯時間：2023 年 7 月 25 日 20：31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaStoreFullAccess

描述：提供所有 MediaStore APIs的完整讀取和寫入存取權

AWSElementalMediaStoreFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSElementalMediaStoreFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 3 月 5 日，UTC 23：15
- 編輯時間：2018 年 3 月 5 日，UTC 23：15
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaStoreReadOnly

描述：提供 MediaStore APIs唯讀許可

AWSElementalMediaStoreReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSElementalMediaStoreReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 3 月 8 日 19：48 UTC
- 編輯時間：2018 年 3 月 8 日 19：48 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaTailorFullAccess

描述：提供 AWS Elemental MediaTailor 資源的完整存取權

`AWSElementalMediaTailorFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSElementalMediaTailorFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 11 月 23 日 00：04 UTC
- 編輯時間：2021 年 11 月 23 日 00：04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSElementalMediaTailorReadOnly

描述：提供 AWS Elemental MediaTailor 資源的唯讀存取權

AWSElementalMediaTailorReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSElementalMediaTailorReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 11 月 23 日 00：05 UTC
- 編輯時間：2021 年 11 月 23 日 00：05 UTC
- ARN: arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSEnhancedClassicNetworkingMangementPolicy

描述：啟用增強型傳統聯網管理功能的政策。

AWSEnhancedClassicNetworkingMangementPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 9 月 20 日 17：29 UTC
- 編輯時間：2017 年 9 月 20 日 17：29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSEntityResolutionConsoleFullAccess

描述：提供 主控台對 AWS 實體解析和相關服務的完整存取權。

AWSEntityResolutionConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSEntityResolutionConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 8 月 17 日 17：54 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:ListInstances",
        "profile:ListDomains",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "profile:ListAccountIntegrations",
        "profile:ListProfileObjectTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "profile:PutProfileObjectType"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/*/object-types/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSEntityResolutionConsoleReadOnlyAccess

描述：透過 提供 AWS 實體解析的唯讀存取權 AWS 管理主控台。

AWSEntityResolutionConsoleReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSEntityResolutionConsoleReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 8 月 17 日 18：18 UTC
- 編輯時間：2023 年 8 月 17 日 18：18 UTC
- ARN: arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSFaultInjectionSimulatorEC2Access

描述：此政策會授予 EC2 和其他必要服務中的 Fault Injection Simulator Service 許可，以執行 FIS 動作。

`AWSFaultInjectionSimulatorEC2Access` 是 AWS 受管政策。

使用此政策

您可以將 `AWSFaultInjectionSimulatorEC2Access` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 10 月 26 日，UTC 20：39
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSFaultInjectionSimulatorECSAccess

描述：此政策會授予 ECS 和其他必要服務中的 Fault Injection Simulator Service 許可，以執行 FIS 動作。

`AWSFaultInjectionSimulatorECSAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSFaultInjectionSimulatorECSAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 10 月 26 日 20：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    },
    {
      "Sid" : "DescribeContainerInstances",
      "Effect" : "Allow",
      "Action" : "ecs:DescribeContainerInstances",
      "Resource" : "arn:aws:ecs:*:*:container-instance/*/*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSFaultInjectionSimulatorEKSAccess

描述：此政策授予 EKS 中的 Fault Injection Simulator Service 許可和其他執行 FIS 動作的必要服務。

`AWSFaultInjectionSimulatorEKSAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSFaultInjectionSimulatorEKSAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 10 月 26 日 20：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSFaultInjectionSimulatorNetworkAccess

描述：此政策會授予 EC2 網路和其他必要服務中的 Fault Injection Simulator Service 許可，以執行 FIS 動作。

`AWSFaultInjectionSimulatorNetworkAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSFaultInjectionSimulatorNetworkAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 10 月 26 日 20：32 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSFaultInjectionSimulatorRDSAccess

描述：此政策會授予 RDS 和其他必要服務中的 Fault Injection Simulator Service 許可，以執行 FIS 動作。

`AWSFaultInjectionSimulatorRDSAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSFaultInjectionSimulatorRDSAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 10 月 26 日 20：30 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC

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

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSFaultInjectionSimulatorSSMAccess

描述：此政策授予 SSM 中的 Fault Injection Simulator Service 許可和其他執行 FIS 動作的必要服務。

`AWSFaultInjectionSimulatorSSMAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSFaultInjectionSimulatorSSMAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 10 月 26 日 15：33 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSFinSpaceServiceRolePolicy

描述：允許存取 AWS 服務 Amazon FinSpace 使用或管理之 資源的政策

AWSFinSpaceServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- **建立時間**：2023 年 5 月 12 日 16：42 UTC
- **編輯時間**：2023 年 12 月 1 日 21：05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSFMAdminFullAccess

描述：FM AWS 管理員的完整存取權

AWSFMAdminFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSFMAdminFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 5 月 9 日 18：06 UTC
- 編輯時間：2022 年 10 月 20 日，UTC 23：39
- ARN: arn:aws:iam::aws:policy/AWSFMAdminFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSFMAdminReadOnlyAccess

描述：FM AWS 管理員的唯讀存取權，允許監控 FM AWS 操作

AWSFMAdminReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSFMAdminReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 5 月 9 日，UTC 20：07

- **編輯時間**：2022 年 10 月 31 日 22：42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSFMMemberReadOnlyAccess

描述：為 AWS Firewall Manager 成員帳戶提供 AWS WAF 動作的唯讀存取權

AWSFMMemberReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSFMMemberReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 5 月 9 日，UTC 21：05
- 編輯時間：2018 年 5 月 9 日，UTC 21：05
- ARN: arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSForWordPressPluginPolicy

描述： AWS For Wordpress 外掛程式的受管政策

AWSForWordPressPluginPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSForWordPressPluginPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 10 月 30 日 00：27 UTC
- 編輯時間：2020 年 1 月 20 日 23：20 UTC
- ARN: arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGitSyncServiceRolePolicy

描述：允許 AWS 程式碼連線從您的 git 儲存庫同步內容的政策

AWSGitSyncServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 16 日 17：05 UTC
- 編輯時間：2024 年 4 月 26 日 18：12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSGlobalAcceleratorSLRPolicy

描述：將許可授予 AWS Global Accelerator 以管理 EC2 彈性網路介面和安全群組的政策。

`AWSGlobalAcceleratorSLRPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 4 月 5 日 19：39 UTC
- 編輯時間：2024 年 10 月 29 日 18：23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "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",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "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/*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGlueConsoleFullAccess

描述：透過 提供 Glue AWS 的完整存取權 AWS 管理主控台

AWSGlueConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSGlueConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 8 月 14 日 13：37 UTC

- **編輯時間**：2023 年 7 月 14 日 14：37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGlueConsoleSageMakerNotebookFullAccess

描述：透過 提供 AWS Glue 的完整存取權， AWS 管理主控台 並存取 sagemaker 筆記本執行個體。

`AWSGlueConsoleSageMakerNotebookFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSGlueConsoleSageMakerNotebookFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 10 月 5 日 17：52 UTC
- 編輯時間：2021 年 7 月 15 日 15：24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AwsGlueDataBrewFullAccessPolicy

描述：透過 提供 Glue DataBrew AWS 的完整存取權 AWS 管理主控台。也提供相關服務的選取存取權（例如 S3、KMS、Glue)。

`AwsGlueDataBrewFullAccessPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AwsGlueDataBrewFullAccessPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 11 月 11 日 16：51 UTC
- 編輯時間：2022 年 2 月 4 日 18：28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGlueDataBrewServiceRole

描述：此政策授予黏附 許可，以對使用者的黏附資料目錄執行動作，此政策也提供 ec2 動作的許可，以允許黏附 建立 ENI 以連接到 VPC 中的資源，也允許黏附 存取 Lakeformation 中註冊的資料，以及存取使用者 cloudwatch 的許可

AWSGlueDataBrewServiceRole 是 AWS 受管政策。

使用此政策

您可以將 AWSGlueDataBrewServiceRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 12 月 4 日 21：26 UTC
- 編輯時間：2024 年 3 月 20 日 23：28 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSGlueSchemaRegistryFullAccess

描述：提供 Glue AWS 結構描述登錄檔服務的完整存取權

AWSGlueSchemaRegistryFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSGlueSchemaRegistryFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 11 月 20 日 00：19 UTC
- 編輯時間：2020 年 11 月 20 日 00：19 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGlueSchemaRegistryReadonlyAccess

描述：提供 Glue AWS 結構描述登錄檔服務的唯讀存取權

AWSGlueSchemaRegistryReadonlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSGlueSchemaRegistryReadonlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 11 月 20 日 00：20 UTC
- 編輯時間：2020 年 11 月 20 日 00：20 UTC
- ARN: arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGlueServiceNotebookRole

描述：Glue AWS 服務角色的政策，允許客戶管理筆記本伺服器

AWSGlueServiceNotebookRole 是 AWS 受管政策。

使用此政策

您可以將 AWSGlueServiceNotebookRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 8 月 14 日 13：37 UTC
- 編輯時間：2023 年 10 月 9 日 15：59 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGlueServiceRole

描述：Glue AWS 服務角色的政策，允許存取相關服務，包括 EC2, S3 和 Cloudwatch Logs

AWSGlueServiceRole 是 AWS 受管政策。

使用此政策

您可以將 AWSGlueServiceRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 8 月 14 日 13：37 UTC

- **編輯時間**：2023 年 9 月 11 日 16：39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AwsGlueSessionUserRestrictedNotebookPolicy

描述：提供許可，允許使用者僅建立和使用與使用者相關聯的筆記本工作階段。此政策也包含明確允許使用者傳遞受限 Glue 工作階段角色的許可。

AwsGlueSessionUserRestrictedNotebookPolicy 是 AWS 受管政策。

使用此政策

您可以將 AwsGlueSessionUserRestrictedNotebookPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 4 月 18 日 15：24 UTC

- **編輯時間**：2024 年 8 月 15 日 20：51 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/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: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*",
        "arn:aws:iam::*:role/AwsGlueSessionUserRestrictedNotebookServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AwsGlueSessionUserRestrictedNotebookServiceRole

描述：提供工作階段以外所有 AWS Glue 資源的完整存取權。允許使用者僅建立並使用與使用者相關聯的筆記本工作階段。此政策也包含 AWS Glue 管理其他服務中的 Glue 資源所需的其他許可 AWS 。

`AwsGlueSessionUserRestrictedNotebookServiceRole` 是 AWS 受管政策。

使用此政策

您可以將 `AwsGlueSessionUserRestrictedNotebookServiceRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 4 月 18 日 15：27 UTC
- 編輯時間：2024 年 8 月 15 日 20：51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/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: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/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AwsGlueSessionUserRestrictedPolicy

描述：提供許可，允許使用者僅建立和使用與使用者相關聯的互動式工作階段。此政策也包含明確允許使用者傳遞受限 Glue 工作階段角色的許可。

AwsGlueSessionUserRestrictedPolicy 是 AWS 受管政策。

使用此政策

您可以將 AwsGlueSessionUserRestrictedPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 4 月 14 日 21：31 UTC
- 編輯時間：2024 年 8 月 5 日 23：06 UTC
- ARN: arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
```

```
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowPassRoleActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AwsGlueSessionUserRestrictedServiceRole

描述：提供工作階段以外所有 AWS Glue 資源的完整存取權。允許使用者建立並僅使用與使用者相關聯的互動式工作階段。此政策也包含 AWS Glue 管理其他服務中的 Glue 資源所需的其他許可 AWS

`AwsGlueSessionUserRestrictedServiceRole` 是 AWS 受管政策。

使用此政策

您可以將 `AwsGlueSessionUserRestrictedServiceRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2022 年 4 月 14 日 21：30 UTC
- 編輯時間：2024 年 8 月 5 日 23：14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
```

```
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
```

```
      }
    },
    {
      "Sid" : "AllowStatementActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessionsAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectCrawlerActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Sid" : "AllowLogsActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Sid" : "AllowTagsActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGrafanaAccountAdministrator

描述：提供 Amazon Grafana 內的存取權，以建立和管理整個組織的工作區。

AWSGrafanaAccountAdministrator 是 AWS 受管政策。

使用此政策

您可以將 AWSGrafanaAccountAdministrator 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 2 月 23 日 00：20 UTC
- 編輯時間：2022 年 2 月 15 日 22：36 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGrafanaConsoleReadOnlyAccess

描述：存取 Amazon Grafana 中的唯讀操作。

`AWSGrafanaConsoleReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSGrafanaConsoleReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 2 月 23 日 00：10 UTC
- 編輯時間：2022 年 2 月 15 日 22：30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSGrafanaWorkspacePermissionManagement

描述：僅提供更新 Grafana AWS 工作區使用者和群組許可的功能。

AWSGrafanaWorkspacePermissionManagement 是 AWS 受管政策。

使用此政策

您可以將 AWSGrafanaWorkspacePermissionManagement 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 2 月 23 日 00：15 UTC
- 編輯時間：2023 年 3 月 15 日 22：17 UTC
- ARN: arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGrafanaWorkspacePermissionManagementV2

描述：提供更新 Amazon Managed Grafana 工作區 IAM Identity Center (IdC) 使用者和群組許可的功能。

AWSGrafanaWorkspacePermissionManagementV2 是 AWS 受管政策。

使用此政策

您可以將 AWSGrafanaWorkspacePermissionManagementV2 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 1 月 5 日 18：39 UTC
- 編輯時間：2024 年 1 月 5 日 18：39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGreengrassFullAccess

描述：此政策提供 AWS Greengrass 組態、管理和部署動作的完整存取權

AWSGreengrassFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSGreengrassFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 5 月 3 日 00：47 UTC
- 編輯時間：2017 年 5 月 3 日 00：47 UTC
- ARN: arn:aws:iam::aws:policy/AWSGreengrassFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGreengrassReadOnlyAccess

描述：此政策提供 AWS Greengrass 組態、管理和部署動作的唯讀存取權

AWSGreengrassReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSGreengrassReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 10 月 30 日 16：01 UTC

- **編輯時間**：2018 年 10 月 30 日 16：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGreengrassResourceAccessRolePolicy

描述： AWS Greengrass 服務角色的政策，允許存取相關服務，包括 AWS Lambda 和 AWS IoT 物件影子。

AWSGreengrassResourceAccessRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSGreengrassResourceAccessRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 2 月 14 日 21：17 UTC
- 編輯時間：2018 年 11 月 14 日 00：35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSGroundStationAgentInstancePolicy

描述：提供使用 AWS Ground Station Agent 的 Dataflow 端點執行個體許可

AWSGroundStationAgentInstancePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSGroundStationAgentInstancePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 3 月 29 日 15：23 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "groundstation:RegisterAgent",
        "groundstation:UpdateAgentStatus",
        "groundstation:GetAgentConfiguration",
        "groundstation:GetAgentTaskResponseUrl"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSHealth_EventProcessorServiceRolePolicy

描述：允許 AWS 運作狀態啟用運作狀態事件處理器功能。

`AWSHealth_EventProcessorServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 1 月 13 日 19：24 UTC
- 編輯時間：2023 年 1 月 13 日 19：24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSHealthFullAccess

描述：允許完整存取 AWS 運作狀態 Apis 和通知以及個人運作狀態儀表板

AWSHealthFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSHealthFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 12 月 6 日 12：30 UTC
- 編輯時間：2020 年 11 月 16 日 18：11 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSHealthImagingFullAccess

描述：提供 AWS Health Imaging 服務的完整存取權。

`AWSHealthImagingFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSHealthImagingFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- 建立時間：2023 年 7 月 25 日，UTC 23：39
- 編輯時間：2023 年 7 月 25 日 23：39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSHealthImagingReadOnlyAccess

描述：提供 AWS Health Imaging 服務的唯讀存取權。

AWSHealthImagingReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSHealthImagingReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 7 月 25 日 23：40 UTC
- 編輯時間：2023 年 8 月 1 日 15：18 UTC
- ARN: arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSHealthImagingServiceRolePolicy

描述：提供 AWS HealthImaging 管理服務操作和發佈服務指標的許可

`AWSHealthImagingServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2026 年 1 月 30 日 18：34 UTC
- 編輯時間：2026 年 1 月 30 日 18：34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthImagingServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSHealthOmicsServiceLinkedRolePolicy

描述：Amazon HealthOmics Service 連結角色的受管政策

AWSHealthOmicsServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2026 年 3 月 4 日 22：57 UTC
- 編輯時間：2026 年 3 月 4 日 22：57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealthOmicsServiceLinkedRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEC2DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowVpcGetActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Service" : "HealthOmics"
        }
      }
    },
    {
      "Sid" : "AllowCreateNetworkInterfaceSubnetSecurityGroup",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowCreateTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowDeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/Service" : "HealthOmics"
        }
      }
    },
    {
      "Sid" : "AllowAssignUnassignPrivateIpAddresses",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "HealthOmics"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIAMIdentityCenterAllowListForIdentityContext

描述：提供使用 IAM Identity Center 身分內容擔任之角色所允許的動作清單。 AWS Security Token Service (AWS STS) 會自動將此政策連接至擔任的角色。身分內容會以 ProvidedContext 形式傳遞。

`AWSIAMIdentityCenterAllowListForIdentityContext` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIAMIdentityCenterAllowListForIdentityContext` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 11 月 8 日 15：21 UTC
- 編輯時間：2024 年 10 月 1 日 14：19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "aoss:APIAccessAll",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
```

```
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:ListSteps",
        "es:ESHttpHead",
        "es:ESHttpPost",
        "es:ESHttpGet",
        "es:ESHttpPatch",
        "es:ESHttpDelete",
        "es:ESHttpPut",
        "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",
        "s3:ListCallerAccessGrants",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "qapps:CreateQApp",
        "qapps:PredictProblemStatementFromConversation",
        "qapps:PredictQAppFromProblemStatement",
        "qapps:CopyQApp",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:UpdateQApp",
        "qapps:DeleteQApp",
        "qapps:AssociateQAppWithUser",
        "qapps:DisassociateQAppFromUser",
        "qapps:ImportDocumentToQApp",
        "qapps:ImportDocumentToQAppSession",
        "qapps:CreateLibraryItem",
        "qapps:GetLibraryItem",
        "qapps:UpdateLibraryItem",
        "qapps:CreateLibraryItemReview",
        "qapps:ListLibraryItems",
        "qapps:CreateSubscriptionToken",
        "qapps:StartQAppSession",
        "qapps:StopQAppSession",
        "qapps:PredictQApp",
        "qapps:ImportDocument",
        "qapps:AssociateLibraryItemReview",
```

```
        "qapps:DisassociateLibraryItemReview",
        "qapps:GetQAppSession",
        "qapps:UpdateQAppSession",
        "qapps:GetQAppSessionMetadata",
        "qapps:UpdateQAppSessionMetadata",
        "qapps:TagResource",
        "qapps:ListQAppSessionData",
        "qapps:ExportQAppSessionData",
        "qbusiness:Chat",
        "qbusiness:ChatSync",
        "qbusiness:ListConversations",
        "qbusiness:ListMessages",
        "qbusiness:DeleteConversation",
        "qbusiness:PutFeedback",
        "sts:SetContext"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIdentityCenterExternalManagementPolicy

描述：提供從外部供應商管理 IAM Identity Center 使用者的存取權。

`AWSIdentityCenterExternalManagementPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIdentityCenterExternalManagementPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 11 月 22 日 00：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIdentityCenterExternalManagementPolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IdentityStoreUserCreation",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:CreateUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false",
          "identitystore:ReservedUserId" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "IdentityStoreUserManagement",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:UpdateUser",
        "identitystore:DeleteUser",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false"
        }
      }
    },
    {
      "Sid" : "IdentityStoreCMKAccess",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : [
            "arn:aws:identitystore::${aws:PrincipalAccount}:identitystore/
${aws:PrincipalTag/IdentityStoreId}"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIdentitySyncFullAccess

描述：授予 Identity Sync 服務的完整存取權

`AWSIdentitySyncFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIdentitySyncFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 3 月 23 日，UTC 23：29
- 編輯時間：2022 年 3 月 23 日 23：29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIdentitySyncReadOnlyAccess

描述：唯讀存取 Identity Sync 服務

AWSIdentitySyncReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIdentitySyncReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 3 月 23 日，UTC 23：29
- 編輯時間：2022 年 3 月 23 日 23：29 UTC
- ARN: arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSImageBuilderFullAccess

描述：提供所有 AWS Image Builder 動作的完整存取權，以及相關 AWS 服務的資源範圍存取權。

AWSImageBuilderFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSImageBuilderFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 20 日 18：25 UTC
- 編輯時間：2021 年 4 月 13 日 17：33 UTC
- ARN: arn:aws:iam::aws:policy/AWSImageBuilderFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSImageBuilderReadOnlyAccess

描述：提供所有 AWS 映像建置器動作的唯讀存取權。

`AWSImageBuilderReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSImageBuilderReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 12 月 19 日，22：29 UTC
- 編輯時間：2019 年 12 月 19 日，22：29 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSImportExportFullAccess

描述：提供對在 下建立之任務的讀取和寫入存取權 AWS 帳戶。

AWSImportExportFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSImportExportFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: arn:aws:iam::aws:policy/AWSImportExportFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSImportExportReadOnlyAccess

描述：提供對在 下建立之任務的唯讀存取權 AWS 帳戶。

`AWSImportExportReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSImportExportReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIncidentManagerIncidentAccessServiceRolePolicy

描述：授予 Incident Manager 呼叫其他服務的許可 AWS ，做為管理事件的一部分。

`AWSIncidentManagerIncidentAccessServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIncidentManagerIncidentAccessServiceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 11 月 13 日 00：01 UTC
- 編輯時間：2024 年 2 月 20 日 23：02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIncidentManagerResolverAccess

描述：此政策授予許可，以啟動、檢視和更新事件，並完整存取自訂時間軸事件和相關項目。將此政策指派給將建立和解決事件的使用者。

AWSIncidentManagerResolverAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIncidentManagerResolverAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 5 月 10 日 06：12 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident",
        "ssm-contacts:StartEngagement"
      ],
      "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIncidentManagerServiceRolePolicy

描述：此政策授予 Incident Manager 代表您管理事件記錄和相關資源的許可。

AWSIncidentManagerServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 5 月 10 日 03：34 UTC
- 編輯時間：2025 年 1 月 28 日 02：52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSIoT1ClickFullAccess

描述：提供 AWS IoT 1-Click 的完整存取權。

`AWSIoT1ClickFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoT1ClickFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2018 年 5 月 11 日，UTC 22：10
- 編輯時間：2018 年 5 月 11 日，UTC 22：10
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoT1ClickReadOnlyAccess

描述：提供 AWS IoT 1-Click 的唯讀存取權。

`AWSIoT1ClickReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 AWSIoT1ClickReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 5 月 11 日，UTC 21：49
- 編輯時間：2018 年 5 月 11 日，UTC 21：49
- ARN: arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTAnalyticsFullAccess

描述：提供 IoT Analytics 的完整存取權。

AWSIoTAnalyticsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTAnalyticsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 6 月 18 日 23：02 UTC
- 編輯時間：2018 年 6 月 18 日 23：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTAnalyticsReadOnlyAccess

描述：提供 IoT Analytics 的唯讀存取權。

`AWSIoTAnalyticsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTAnalyticsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 6 月 18 日 21：37 UTC
- 編輯時間：2018 年 6 月 18 日 21：37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTConfigAccess

描述：此政策提供 AWS IoT 組態動作的完整存取權

AWSIoTConfigAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTConfigAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 10 月 27 日，UTC 21：52
- 編輯時間：2019 年 9 月 27 日，UTC 20：48
- ARN: arn:aws:iam::aws:policy/AWSIoTConfigAccess

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTConfigReadOnlyAccess

描述：此政策提供 IoT AWS IoT 組態動作的唯讀存取權

`AWSIoTConfigReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTConfigReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 10 月 27 日，UTC 21：52
- 編輯時間：2019 年 9 月 27 日，UTC 20：52
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTDataAccess

描述：此政策提供 AWS IoT 訊息動作的完整存取權

AWSIoTDataAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTDataAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 10 月 27 日，UTC 21：51
- 編輯時間：2021 年 6 月 23 日，UTC 21：34
- ARN: arn:aws:iam::aws:policy/AWSIoTDataAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

描述：提供 IoT 物件群組的寫入存取權和 IoT 憑證的讀取存取權，以執行 ADD_THINGS_TO_THING_GROUP 緩解動作

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 8 月 7 日 17：55 UTC
- 編輯時間：2019 年 8 月 7 日 17：55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTDeviceDefenderAudit

描述：提供 IoT 和相關資源的讀取存取權

AWSIoTDeviceDefenderAudit 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTDeviceDefenderAudit 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 7 月 18 日 21：17 UTC
- 編輯時間：2019 年 11 月 25 日，UTC 23：52
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

描述：提供啟用 IoT 記錄以執行 ENABLE_IOT_LOGGING 緩解動作的存取權

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 8 月 7 日 17：04 UTC
- 編輯時間：2019 年 8 月 7 日 17：04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

描述：提供訊息發佈 SNS 主題的存取權，以執行 PUBLISH_FINDING_TO_SNS 緩解動作

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 8 月 7 日 17：04 UTC
- 編輯時間：2019 年 8 月 7 日 17：04 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

描述：提供 IoT 政策的寫入存取權，以執行 REPLACE_DEFAULT_POLICY_VERSION 緩解動作

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 8 月 7 日 17：04 UTC
- 編輯時間：2019 年 8 月 7 日 17：04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTDeviceDefenderUpdateCACertMitigationAction

描述：提供 IoT CA 憑證的寫入存取權，以執行 UPDATE_CA_CERTIFICATE 緩解動作

`AWSIoTDeviceDefenderUpdateCACertMitigationAction` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTDeviceDefenderUpdateCACertMitigationAction` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 8 月 7 日 17：05 UTC

- **編輯時間**：2019 年 8 月 7 日 17：05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

描述：提供 IoT 憑證的寫入存取權，以執行 UPDATE_DEVICE_CERTIFICATE 緩解動作

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 8 月 7 日 17：06 UTC
- 編輯時間：2019 年 8 月 7 日 17：06 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTDeviceTesterForFreeRTOSFullAccess

描述：允許 AWS IoT Device Tester 透過允許存取 IoT、S3 和 IAM 等服務來執行 FreeRTOS 資格套件

`AWSIoTDeviceTesterForFreeRTOSFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTDeviceTesterForFreeRTOSFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 2 月 12 日 20：33 UTC
- 編輯時間：2023 年 8 月 10 日 20：30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTDeviceTesterForGreengrassFullAccess

描述：允許 AWS IoT Device Tester 執行 AWS Greengrass 資格套件，方法是允許存取相關服務，包括 Lambda、IoT、API Gateway、IAM

`AWSIoTDeviceTesterForGreengrassFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTDeviceTesterForGreengrassFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 2 月 20 日 21：21 UTC
- 編輯時間：2020 年 6 月 25 日 17：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTEventsFullAccess

描述：提供 IoT Events 的完整存取權。

AWSIoTEventsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTEventsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 1 月 10 日 22：51 UTC
- 編輯時間：2019 年 1 月 10 日 22：51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTEventsReadOnlyAccess

描述：提供 IoT Events 的唯讀存取權。

AWSIoTEventsReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTEventsReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 1 月 10 日 22：50 UTC
- 編輯時間：2019 年 9 月 23 日 17：22 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTFleetHubFederationAccess

描述：IoT Fleet Hub 應用程式的聯合存取

`AWSIoTFleetHubFederationAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTFleetHubFederationAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 12 月 15 日 08：08 UTC
- 編輯時間：2022 年 4 月 4 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTFleetwiseServiceRolePolicy

描述：授予 AWSIoTFleetwise 用於輔助功能 AWS 的資源和 metaData 的許可

AWSIoTFleetwiseServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 9 月 21 日，UTC 23：27
- 編輯時間：2025 年 10 月 16 日 04：04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTFullAccess

描述：此政策提供 AWS IoT 組態和簡訊動作的完整存取權

AWSIoTFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 10 月 8 日 15：19 UTC
- 編輯時間：2022 年 5 月 19 日，UTC 21：39
- ARN: arn:aws:iam::aws:policy/AWSIoTFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTLogging

描述：允許建立 Amazon CloudWatch Log 群組和將日誌串流至群組

AWSIoTLogging 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTLogging 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 10 月 8 日 15：17 UTC
- 編輯時間：2015 年 10 月 8 日 15：17 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTLogging

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTManagedIntegrationsFullAccess

描述：提供 AWS IoT 裝置管理和相關服務的受管整合的完整存取權。

AWSIoTManagedIntegrationsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTManagedIntegrationsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 3 月 5 日 19：22 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTManagedIntegrationsFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iotmanagedintegrations:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
iotmanagedintegrations.amazonaws.com/AWSServiceRoleForIoTManagedIntegrations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotmanagedintegrations.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTManagedIntegrationsRolePolicy

描述：提供 IoT AWS IoT 裝置管理的受管整合許可，以代表您發佈日誌和指標。

`AWSIoTManagedIntegrationsRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 3 月 5 日 21：22 UTC
- 編輯時間：2025 年 3 月 5 日 21：22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTManagedIntegrationsRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTManagedIntegrations",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSIoTOTAUpdate

描述：允許存取 create AWS IoT 任務並描述 AWS 程式碼簽署者任務

`AWSIoTOTAUpdate` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTOTAUpdate` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 12 月 20 日，UTC 20：36
- 編輯時間：2017 年 12 月 20 日，UTC 20：36
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIotRoboRunnerFullAccess

描述：此政策會授予許可，以允許完整存取 AWS Iot RoboRunner。

`AWSIotRoboRunnerFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIotRoboRunnerFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 29 日 03：54 UTC

- **編輯時間**：2023 年 2 月 23 日 18：34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIotRoboRunnerReadOnly

描述：此政策授予許可，允許對 AWS Iot RoboRunner 進行唯讀存取。

AWSIotRoboRunnerReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSIotRoboRunnerReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 29 日 03：43 UTC
- 編輯時間：2022 年 11 月 16 日 20：51 UTC
- ARN: arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIotRoboRunnerServiceRolePolicy

描述：允許 AWS IoT RoboRunner 代表客戶管理相關聯的 AWS 資源。

`AWSIotRoboRunnerServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 2 月 21 日 16：56 UTC
- 編輯時間：2023 年 2 月 21 日 16：56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSIoTRuleActions

描述：允許存取 AWS IoT 規則動作中支援的所有 AWS 服務

AWSIoTRuleActions 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTRuleActions 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 10 月 8 日 15：14 UTC

- **編輯時間**：2018 年 1 月 16 日 19：28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTSiteWiseConsoleFullAccess

描述：提供使用 管理 AWS IoT SiteWise 的完整存取權 AWS 管理主控台。請注意，此政策也授予建立和列出與 AWS IoT SiteWise （ 例如 AWS IoT Analytics) 搭配使用之資料存放區的存取權、列出和檢視 AWS IoT Greengrass 資源的存取權、列出和修改 AWS Secrets Manager 秘密、擷取 AWS IoT 物件影子、列出具有特定標籤的資源，以及建立和使用 AWS IoT SiteWise 的服務連結角色。

`AWSIoTSiteWiseConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTSiteWiseConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 5 月 31 日 21：37 UTC
- 編輯時間：2019 年 5 月 31 日 21：37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

政策版本

政策版本： v1 （ 預設 ）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTSiteWiseFullAccess

描述：提供 IoT SiteWise 的完整存取權。

AWSIoTSiteWiseFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTSiteWiseFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 12 月 4 日，UTC 20：53
- 編輯時間：2018 年 12 月 4 日，UTC 20：53
- ARN: arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTSiteWiseMonitorPortalAccess

描述：此政策授予存取 AWS IoT SiteWise 資產和資產資料的許可、建立 AWS IoT SiteWise Monitor 資源，以及列出 AWS SSO 使用者。

`AWSIoTSiteWiseMonitorPortalAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTSiteWiseMonitorPortalAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 5 月 19 日，20：01 UTC
- 編輯時間：2020 年 5 月 19 日，20：01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTSiteWiseMonitorServiceRolePolicy

描述：此角色授與 AWS IoT SiteWise 監控存取 AWS IoT SiteWise 資產和資產屬性的許可，以及透過 AWS IoT SiteWise 入口網站建立 AWS IoT Sitewise 專案、儀表板和存取政策。

`AWSIoTSiteWiseMonitorServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 14 日 00：59 UTC
- 編輯時間：2019 年 12 月 13 日 22：19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSIoTSiteWiseReadOnlyAccess

描述：提供 IoT SiteWise 的唯讀存取權。

`AWSIoTSiteWiseReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTSiteWiseReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 12 月 4 日，UTC 20：55
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:BatchGetAssetPropertyAggregates",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValueHistory",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAction",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetCompositeModel",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelInterfaceRelationship",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:DescribeBulkImportJob",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeComputationModelExecutionSummary",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
        "iotsitewise:DescribeDefaultEncryptionConfiguration",
        "iotsitewise:DescribeExecution",
        "iotsitewise:DescribeGateway",
```

```
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:DescribeLoggingOptions",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:DescribeStorageConfiguration",
        "iotsitewise:DescribeTimeSeries",
        "iotsitewise:ExecuteQuery",
        "iotsitewise:GetAssetPropertyAggregates",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetInterpolatedAssetPropertyValues",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListActions",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssetRelationships",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListBulkImportJobs",
        "iotsitewise:ListCompositionRelationships",
        "iotsitewise:ListComputationModelDataBindingUsages",
        "iotsitewise:ListComputationModelResolveToResources",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListExecutions",
        "iotsitewise:ListGateways",
        "iotsitewise:ListInterfaceRelationships",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iotsitewise:ListTimeSeries"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTThingsRegistration

描述：此政策允許使用者使用 AWS IoT StartThingRegistrationTask API 大量註冊物件

AWSIoTThingsRegistration 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTThingsRegistration 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 12 月 1 日 20：21 UTC
- 編輯時間：2020 年 10 月 5 日 19：20 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTTwinMakerServiceRolePolicy

描述：允許 AWS IoT TwinMaker 呼叫其他 AWS 服務，並代表您同步其資源。

AWSIoTTwinMakerServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 13 日 18：59 UTC
- 編輯時間：2023 年 11 月 13 日 18：59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSIoTWirelessDataAccess

描述：允許相關聯的身分資料存取 AWS IoT Wireless 裝置。

AWSIoTWirelessDataAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTWirelessDataAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 15 日 15：31 UTC
- 編輯時間：2020 年 12 月 15 日 15：31 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTWirelessFullAccess

描述：允許關聯身分完整存取 all AWS IoT Wireless 操作。

`AWSIoTWirelessFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTWirelessFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 15 日 15：27 UTC
- 編輯時間：2020 年 12 月 15 日 15：27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTWirelessFullPublishAccess

描述：提供 IoT Wireless 代表您發佈至 IoT 規則引擎的完整存取權。

`AWSIoTWirelessFullPublishAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTWirelessFullPublishAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 15 日 15：29 UTC
- 編輯時間：2020 年 12 月 15 日 15：29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTWirelessGatewayCertManager

描述：允許相關聯的身分存取建立、列出和描述 IoT 憑證

AWSIoTWirelessGatewayCertManager 是 AWS 受管政策。

使用此政策

您可以將 AWSIoTWirelessGatewayCertManager 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 15 日 15：30 UTC
- 編輯時間：2020 年 12 月 15 日 15：30 UTC
- ARN: arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIoTWirelessLogging

描述：允許相關聯的身分建立 Amazon CloudWatch Logs 群組，並將日誌串流至群組。

`AWSIoTWirelessLogging` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTWirelessLogging` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 15 日 15：32 UTC
- 編輯時間：2020 年 12 月 15 日 15：32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIoTWirelessReadOnlyAccess

描述：允許相關聯的身分唯讀存取 AWS IoT 無線。

`AWSIoTWirelessReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSIoTWirelessReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 15 日 15：28 UTC
- 編輯時間：2020 年 12 月 15 日 15：28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSIPAMServiceRolePolicy

描述：允許 VPC IP Address Manager 代表您存取 VPC 資源並與 AWS Organizations 整合。

`AWSIPAMServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 30 日 19：08 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListDistributionsByAnycastIpListId",
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    },
    {
      "Sid" : "IPAMAllocationPolicyActions",
      "Effect" : "Allow",
      "Action" : "ec2:AllocateIpamPoolCidr",
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListResolverWriteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:Attribute/ExpectedIpamPrefixListResolverTarget" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "PrefixListResolverReadActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSIQContractServiceRolePolicy

描述： AWS IQ 用來代表客戶執行付款請求

AWSIQContractServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 8 月 22 日 19：28 UTC
- 編輯時間：2019 年 8 月 22 日 19：28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIQFullAccess

描述：提供 AWS IQ 的完整存取權

AWSIQFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSIQFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 4 月 4 日，UTC 23：13
- 編輯時間：2019 年 9 月 25 日，UTC 20：22
- ARN: arn:aws:iam::aws:policy/AWSIQFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSIQPermissionServiceRolePolicy

描述：允許 AWS IQ 管理 AWS IQ 專家擔任的角色。

AWSIQPermissionServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 8 月 22 日 19：36 UTC
- 編輯時間：2019 年 8 月 22 日 19：36 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

描述：允許存取 AWS KMS 自訂金鑰存放區所需的 AWS 服務和資源

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 14 日 20：10 UTC
- 編輯時間：2023 年 11 月 10 日 19：03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

描述：讓 AWS KMS 同步多區域金鑰的共用屬性。

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 6 月 16 日 15：37 UTC
- 編輯時間：2024 年 11 月 13 日 22：53 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "kms:SynchronizeMultiRegionKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSKeyManagementServicePowerUser

描述：提供 AWS Key Management Service (KMS) 的存取權。

`AWSKeyManagementServicePowerUser` 是 AWS 受管政策。

使用此政策

您可以將 `AWSKeyManagementServicePowerUser` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2017 年 3 月 7 日 00：55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLakeFormationCrossAccountManager

描述：透過 Lake Formation 提供 Glue 資源的跨帳戶存取權。同時授予其他必要服務的讀取存取權，例如組織和資源存取管理員

`AWSLakeFormationCrossAccountManager` 是 AWS 受管政策。

使用此政策

您可以將 AWSLakeFormationCrossAccountManager 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 8 月 4 日，UTC 20：59
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowManageResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowXAcctManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLakeFormationDataAdmin

描述：授予 AWS Lake Formation 和相關服務的管理存取權，例如 AWS Glue，以管理資料湖

`AWSLakeFormationDataAdmin` 是 AWS 受管政策。

使用此政策

您可以將 `AWSLakeFormationDataAdmin` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 8 月 8 日 17：33 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:CreateCatalog",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
```

```
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSLakeFormationDataAdminDeny",
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambda_FullAccess

描述：授予 AWS Lambda 服務、 AWS Lambda 主控台功能和其他相關 AWS 服務的完整存取權。

`AWSLambda_FullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSLambda_FullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 11 月 17 日 21：14 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "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",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lambda.amazonaws.com/
AWSServiceRoleForLambda",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambda_ReadOnlyAccess

描述：授予對 AWS Lambda 服務、 AWS Lambda 主控台功能和其他相關 AWS 服務的唯讀存取權。

AWSLambda_ReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSLambda_ReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 11 月 17 日 21：10 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaBasicDurableExecutionRolePolicy

描述：提供 CloudWatch Logs 的寫入許可，以及 Lambda 耐用函數使用的耐久執行 APIs讀取/寫入許可

AWSLambdaBasicDurableExecutionRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaBasicDurableExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 12 月 2 日 15：04 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "lambda:CheckpointDurableExecution",
        "lambda:GetDurableExecutionState"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaBasicExecutionRole

描述：提供 CloudWatch Logs 的寫入許可。

AWSLambdaBasicExecutionRole 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaBasicExecutionRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策

- 建立時間：2015 年 4 月 9 日 15：03 UTC
- 編輯時間：2015 年 4 月 9 日 15：03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaDynamoDBExecutionRole

描述：提供 DynamoDB 串流的清單和讀取存取權，以及將許可寫入 CloudWatch 日誌。

AWSLambdaDynamoDBExecutionRole 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaDynamoDBExecutionRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 4 月 9 日 15：09 UTC
- 編輯時間：2015 年 4 月 9 日 15：09 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaENIManagementAccess

描述：提供 Lambda 函數管理已啟用 VPC 的 Lambda 函數所使用的 ENIs（建立、描述、刪除）的最低許可。

AWSLambdaENIManagementAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaENIManagementAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 12 月 6 日 00：37 UTC
- 編輯時間：2020 年 10 月 1 日，UTC 20：07
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaExecute

描述：提供 Put、存取 S3 和完整存取 CloudWatch Logs。

`AWSLambdaExecute` 是 AWS 受管政策。

使用此政策

您可以將 `AWSLambdaExecute` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSLambdaFullAccess

描述：此政策位於棄用路徑上。如需指引，請參閱 文件：https：//https://docs.aws.amazon.com/lambda/latest/dg/access-control-identity-based.html。提供 Lambda、S3、DynamoDB、CloudWatch 指標和日誌的完整存取權。

AWSLambdaFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2017 年 11 月 27 日 23：22 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaFullAccess

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSLambdaInvocation-DynamoDB

描述：提供 DynamoDB Streams 的讀取存取權。

AWSLambdaInvocation-DynamoDB 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaInvocation-DynamoDB 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2015 年 2 月 6 日 18：40 UTC
- ARN: arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSLambdaKinesisExecutionRole

描述：提供 Kinesis 串流的清單和讀取存取權，以及寫入 CloudWatch 日誌的許可。

`AWSLambdaKinesisExecutionRole` 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaKinesisExecutionRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 4 月 9 日 15：14 UTC
- 編輯時間：2018 年 11 月 19 日，UTC 20：09
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSLambdaManagedEC2ResourceOperator

描述：此政策授予 許可，以建立和管理由 Lambda 受管執行個體管理的 EC2 資源，以及描述性許可。

`AWSLambdaManagedEC2ResourceOperator` 是 AWS 受管政策。

使用此政策

您可以將 `AWSLambdaManagedEC2ResourceOperator` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 30 日 08：34 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaManagedEC2ResourceOperator`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : "amazon"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaMSKExecutionRole

描述：提供在 VPC 內存取 MSK 叢集、在 VPC 中管理 ENIs（建立、描述、刪除）以及將許可寫入 CloudWatch Logs 所需的許可。

`AWSLambdaMSKExecutionRole` 是 AWS 受管政策。

使用此政策

您可以將 `AWSLambdaMSKExecutionRole` 連接至使用者、群組與角色。

政策詳細資訊

- **類型**：服務角色政策
- **建立時間**：2020 年 8 月 11 日 17：35 UTC
- **編輯時間**：2022 年 8 月 2 日，UTC 20：08

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

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaReplicator

描述：授予 Lambda Replicator 跨區域複寫函數的必要許可

AWSLambdaReplicator 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 5 月 23 日 17：53 UTC
- 編輯時間：2017 年 12 月 8 日 00：17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaRole

描述： AWS Lambda 服務角色的預設政策。

AWSLambdaRole 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaRole

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSLambdaServiceRolePolicy

描述：允許 Lambda 代表您描述和終止來自 EC2 的受管執行個體。

AWSLambdaServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 11 月 30 日 08：04 UTC
- 編輯時間：2025 年 11 月 30 日 08：04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLambdaServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaSQSQueueExecutionRole

描述：提供 SQS 佇列的接收訊息、刪除訊息和讀取屬性存取權，以及將許可寫入 CloudWatch 日誌。

AWSLambdaSQSQueueExecutionRole 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaSQSQueueExecutionRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策

- **建立時間**：2018 年 6 月 14 日 21：50 UTC
- **編輯時間**：2018 年 6 月 14 日 21：50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLambdaVPCAccessExecutionRole

描述：提供 Lambda 函數在存取 VPC 中的資源時執行的最低許可 - 建立、描述、刪除網路介面，以及將許可寫入 CloudWatch Logs。

AWSLambdaVPCAccessExecutionRole 是 AWS 受管政策。

使用此政策

您可以將 AWSLambdaVPCAccessExecutionRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 2 月 11 日 23：15 UTC
- 編輯時間：2024 年 1 月 5 日 22：38 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLicenseManagerConsumptionPolicy

描述：提供許可，以允許存取使用者有權使用的授權所需的 AWS License Manager API 動作。

`AWSLicenseManagerConsumptionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSLicenseManagerConsumptionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 8 月 11 日 23：18 UTC
- 編輯時間：2021 年 8 月 11 日 23：18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

描述：允許 AWS License Manager Linux Subscriptions Service 代表您管理資源。

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- **建立時間**：2022 年 12 月 20 日 18：54 UTC
- **編輯時間**：2024 年 7 月 8 日 22：04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ]
    }
  ]
```

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLicenseManagerMasterAccountRolePolicy

Description： AWS License Manager 服務主帳戶角色政策

`AWSLicenseManagerMasterAccountRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 26 日 19：03 UTC
- 編輯時間：2022 年 5 月 31 日 20：50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLicenseManagerMemberAccountRolePolicy

Description： AWS License Manager 服務成員帳戶角色政策

AWSLicenseManagerMemberAccountRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 26 日 19：04 UTC
- 編輯時間：2019 年 11 月 15 日，UTC 22：09
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSLicenseManagerServiceRolePolicy

Description： AWS License Manager 服務預設角色政策

AWSLicenseManagerServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 26 日 19：02 UTC
- 編輯時間：2025 年 11 月 19 日 18：34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*::document/AWSLicenseManager-*"
      ]
    },
    {
      "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

描述：允許 AWS License Manager User Subscriptions Service 代表您管理資源。

AWSLicenseManagerUserSubscriptionsServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 7 月 30 日 01：17 UTC
- 編輯時間：2024 年 11 月 8 日 02：54 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
            "bz0vcy31ooqlzk5tsash4r1ik",
            "d44g89hc0gp9jdzm99rznthpw",
            "77yzkpa7kvee1y1tt7wnsdwoc",
            "a8jthu9h8pjsn4b8ylvfl6sfr",
            "7at6der8hnlov1g347e6tdkde",
            "3t0v0vuhvxjzm6m462f9v8iz4",
            "4gs2prcp03ojilgkjx8m3ifh7"
          ]
        }
      },
      "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"
        }
      }
    },
    {
      "Sid" : "ReadHostedZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecurityGroupRulePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Sid" : "DescribeSubnetsPermissions",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:license-manager-user-*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSM2ServicePolicy

描述：允許 AWS M2 代表您管理 AWS 資源。

AWSM2ServicePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 6 月 7 日 20：26 UTC
- 編輯時間：2022 年 6 月 7 日 20：26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSManagedServices_ContactsServiceRolePolicy

描述：允許 AWS Managed Services 讀取 AWS 資源上的標籤值

AWSManagedServices_ContactsServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 3 月 23 日 17：07 UTC
- 編輯時間：2023 年 3 月 23 日 17：07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "tag:GetResources",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetBucketTagging",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:authType" : "REST-HEADER",
          "s3:signatureversion" : "AWS4-HMAC-SHA256"
        },
        "NumericGreaterThanEquals" : {
          "s3:TlsVersion" : "1.2"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

描述： AWS 受管服務 - 管理偵測控制基礎設施的政策

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 12 月 19 日 23：11 UTC
- 編輯時間：2022 年 12 月 19 日 23：11 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSManagedServices_EventsServiceRolePolicy

Description： AWS Managed Services 政策，以啟用 AMS 事件處理器功能。

AWSManagedServices_EventsServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 2 月 7 日 18：41 UTC
- 編輯時間：2023 年 2 月 7 日 18：41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy

描述：允許 Amazon AWS Managed Service 的自助服務報告功能代表您讀取 AWS 組織資料，以啟用組織層級彙總報告

`AWSManagedServices_SelfServiceReporting_ServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 1 月 8 日 21：22 UTC
- 編輯時間：2025 年 1 月 8 日 21：22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSManagedServicesDeploymentToolkitPolicy

描述：允許 AWS Managed Services 代表您管理部署工具組。

`AWSManagedServicesDeploymentToolkitPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 6 月 9 日 18：33 UTC
- 編輯時間：2024 年 4 月 4 日 20：41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AMSCDKToolkitS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
```

```
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitCloudFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:GetTemplateSummary",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitECRPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:CreateRepository",
        "ecr:DeleteLifecyclePolicy",
        "ecr:DeleteRepository",
        "ecr:DeleteRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",
        "ecr:PutImageScanningConfiguration",
        "ecr:PutImageTagMutability",
        "ecr:PutLifecyclePolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSManagementConsoleAdministratorAccess

描述：提供設定和自訂 的完整存取權 AWS 管理主控台

AWSManagementConsoleAdministratorAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSManagementConsoleAdministratorAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：任務函數政策
- 建立時間：2025 年 8 月 14 日 21：19 UTC

- **編輯時間**：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AWSManagementConsoleAdministratorAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:PutAccountColor",
        "uxc:DeleteAccountColor",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
```

```
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListManagedNotificationChildEvents",
        "notifications:ListManagedNotificationConfigurations",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:DeleteEnvironment",
        "cloudshell:GetFileDownloadUrls",
        "cloudshell:GetFileUploadUrls",
        "cloudshell:DescribeEnvironments",
        "cloudshell:PutCredentials",
        "cloudshell:StartEnvironment",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
```

```
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSManagementConsoleBasicUserAccess

描述：授予非管理使用者存取基本 AWS 管理主控台 功能和使用者體驗 (UX) 功能的權限。

`AWSManagementConsoleBasicUserAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSManagementConsoleBasicUserAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2025 年 8 月 14 日 20：34 UTC
- 編輯時間：2026 年 3 月 17 日 22：12 UTC
- ARN: arn:aws:iam::aws:policy/AWSManagementConsoleBasicUserAccess

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:GetAccountCustomizations",
        "uxc:ListServices",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationEvent",
        "notifications:ListManagedNotificationChildEvents",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:StartEnvironment",
        "cloudshell:DeleteEnvironment",
        "cloudshell:PutCredentials",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
```

```
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMarketplaceAmiIngestion

描述：允許 AWS Marketplace 複製您的 Amazon Machine Image AMIs) 以列出它們 AWS Marketplace

`AWSMarketplaceAmiIngestion` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMarketplaceAmiIngestion` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 9 月 25 日，UTC 20：55
- 編輯時間：2020 年 9 月 25 日，UTC 20：55
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

政策版本

政策版本： v1 （ 預設 ）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceDeploymentServiceRolePolicy

描述：允許 為您訂閱的產品 AWS Marketplace 建立和管理賣方部署參數 AWS Marketplace。

AWSMarketplaceDeploymentServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 15 日 23：34 UTC
- 編輯時間：2023 年 11 月 15 日 23：34 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceFullAccess

描述：提供訂閱和取消訂閱 AWS Marketplace 軟體的功能，允許使用者從 Marketplace 'Your Software' 頁面管理 Marketplace 軟體執行個體，並提供 EC2 的管理存取權。

`AWSMarketplaceFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMarketplaceFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 11 日 17：21 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceGetEntitlements

描述：提供 AWS Marketplace 權限的讀取存取權

`AWSMarketplaceGetEntitlements` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMarketplaceGetEntitlements` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 3 月 27 日 19：37 UTC
- 編輯時間：2024 年 4 月 5 日 01：27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceImageBuildFullAccess

描述：提供 AWS Marketplace 私有映像建置功能的完整存取權。除了建立私有映像之外，它還提供將標籤新增至映像、啟動和終止 ec2 執行個體的許可。

AWSMarketplaceImageBuildFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSMarketplaceImageBuildFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 7 月 31 日 23：29 UTC
- 編輯時間：2022 年 3 月 4 日 17：05 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceLicenseManagementServiceRolePolicy

描述：允許存取 AWS Marketplace AWS 服務 和 用於授權管理的資源。

`AWSMarketplaceLicenseManagementServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 3 日，UTC 08：33
- 編輯時間：2020 年 12 月 3 日，UTC 08：33
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceManageSubscriptions

描述：提供訂閱和取消訂閱 AWS Marketplace 軟體的功能

`AWSMarketplaceManageSubscriptions` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMarketplaceManageSubscriptions` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:UpdatePurchaseOrders",
        "aws-marketplace:ListAgreementCharges",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:AcceptAgreementPaymentRequest",
        "aws-marketplace:RejectAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "Null" : {
          "aws-marketplace:AgreementType" : "false"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
    },
    {
      "Sid" : "AWSMarketplaceTokenManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AgentTokenContainer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateAgentTokenContainer",
            "RequestExpressPrivateOffer",
            "ExpireToken"
          ]
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceEntityReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMarketplaceMeteringFullAccess

描述：提供 AWS Marketplace 計量的完整存取權。

`AWSMarketplaceMeteringFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMarketplaceMeteringFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2016 年 3 月 17 日，UTC 22：39
- 編輯時間：2016 年 3 月 17 日，UTC 22：39
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceMeteringRegisterUsage

描述：提供透過 AWS Marketplace Metering Service 註冊資源和追蹤用量的許可。

AWSMarketplaceMeteringRegisterUsage 是 AWS 受管政策。

使用此政策

您可以將 AWSMarketplaceMeteringRegisterUsage 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 11 月 21 日 01：17 UTC
- 編輯時間：2019 年 11 月 21 日 01：17 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceProcurementSystemAdminFullAccess

描述：提供 an AWS Marketplace eProcurement 整合的所有管理動作的完整存取權。

`AWSMarketplaceProcurementSystemAdminFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMarketplaceProcurementSystemAdminFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 6 月 25 日 13：07 UTC
- 編輯時間：2019 年 6 月 25 日 13：07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplacePurchaseOrdersServiceRolePolicy

描述：允許 AWS Marketplace 服務存取採購訂單管理。

`AWSMarketplacePurchaseOrdersServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 10 月 27 日 15：12 UTC
- 編輯時間：2021 年 10 月 27 日 15：12 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceRead-only

描述：提供檢閱 AWS Marketplace 訂閱的功能

`AWSMarketplaceRead-only` 是 AWS 受管政策。

使用此政策

您可以將 AWSMarketplaceRead-only 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceRead-only

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:ListAgreementCharges",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMarketplaceResaleAuthorizationServiceRolePolicy

描述：允許存取 AWS Marketplace AWS 服務 和 用於轉售授權的 使用或管理的資源。

`AWSMarketplaceResaleAuthorizationServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 3 月 5 日 18：47 UTC
- 編輯時間：2025 年 8 月 1 日 15：19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:*:*:*/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" : "AllowResaleAuthorizationShareActionsRAMAcceptDelete",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:DeleteResourceShare"
      ],
      "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",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSMarketplaceSellerFullAccess

描述：提供對 AWS Marketplace 和其他 AWS 服務的所有賣方操作的完整存取權，例如 AMI 管理。

AWSMarketplaceSellerFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSMarketplaceSellerFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 7 月 2 日 20：40 UTC
- 編輯時間：2026 年 3 月 2 日 23：42 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess

政策版本

政策版本： v25 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
```

```
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:GetSellerDashboard",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "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",
        "tax:ListSupplementalTaxRegistrations",
        "tax:PutSupplementalTaxRegistration",
        "tax:DeleteSupplementalTaxRegistration",
        "tax:GetTaxRegistration"
      ],
      "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"
        }
      }
    },
    {
      "Sid" : "AgreementPaymentRequestAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-marketplace:SendAgreementPaymentRequest",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:CancelAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMarketplaceSellerOfferManagement

描述：提供賣方對優惠和協議管理活動的存取權。

AWSMarketplaceSellerOfferManagement 是 AWS 受管政策。

使用此政策

您可以將 AWSMarketplaceSellerOfferManagement 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 19 日 00：41 UTC
- 編輯時間：2024 年 11 月 19 日 00：41 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerOfferManagement

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOfferManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceCreateOfferOnProduct",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : "CreateOfferOnProduct"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceListEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntitiesReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
```

```
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ContainerProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProfessionalServicesProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/SaaSProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AmiProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMarketplaceSellerProductsFullAccess

描述：為賣方提供 AWS Marketplace Management Products 頁面和其他 AWS 服務的完整存取權，例如 AMI 管理。

AWSMarketplaceSellerProductsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSMarketplaceSellerProductsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 7 月 2 日 21：06 UTC
- 編輯時間：2026 年 2 月 19 日 19：12 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListAssessments"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "MarketplaceResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceAssessmentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeAssessment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetIAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsightsAccess",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "ResourceSharingAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-files/
${aws:PrincipalAccount}/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "TechnicalStaff"
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMarketplaceSellerProductsReadOnly

描述：提供賣方對 AWS Marketplace Management Products 頁面的唯讀存取權。

AWSMarketplaceSellerProductsReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSMarketplaceSellerProductsReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 7 月 2 日 21：40 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
```

```
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMcpServiceActionsFullAccess

描述：提供所有 MCP 服務動作的完整存取權。此政策不會授予 MCP 所採取動作的存取權，只會授予 MCP 動作本身的存取權。

AWSMcpServiceActionsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSMcpServiceActionsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 21 日，UTC 22：49
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMcpServiceActionsFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllMCPServiceActions",
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMediaConnectServicePolicy

描述：啟用 MediaConnect 使用或管理之 AWS 服務 資源存取權的預設政策。

AWSMediaConnectServicePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 4 月 3 日 22：11 UTC
- 編輯時間：2025 年 10 月 29 日，UTC 21：34
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/created-for-service" : "MediaConnect"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMediaLiveAnywhereServiceRolePolicy

描述：允許 MediaLive Anywhere 代表您建立和管理 AWS 資源。

AWSMediaLiveAnywhereServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- **建立時間**：2025 年 4 月 14 日，UTC 22：07
- **編輯時間**：2025 年 4 月 14 日 22：07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaLiveAnywhereServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PutMediaLiveMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MediaLive"
        }
      }
    },
    {
      "Sid" : "RegisterAnywhereAgentTaskDefinition",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        }
```

```
      }
    },
    {
      "Sid" : "ECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : "RegisterTaskDefinition",
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "created_by"
        }
      }
    },
    {
      "Sid" : "UpdateAnywhereAgentService",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*",
          "ecs:Task-Definition" : "arn:aws:ecs:*:*:task-definition/
MediaLiveAnywhereAgent*"
        }
      }
    },
    {
      "Sid" : "ECSListTaskDefinitions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTaskDefinitions"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeregisterAnywhereAgentTaskDefinitionOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeregisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentTaskDefinitionsOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteTaskDefinitions"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentServiceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:service/MediaLiveAnywhere*/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
        }
      }
    },
    {
      "Sid" : "DeregisterContainerInstanceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListContainerInstances",
```

```
        "ecs:DeregisterContainerInstance"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSMediaTailorServiceRolePolicy

描述：啟用存取 MediaTailor 使用或管理 AWS 的資源

AWSMediaTailorServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 9 月 17 日，UTC 22：27
- 編輯時間：2021 年 9 月 17 日，22：27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMigrationHubDiscoveryAccess

描述：政策允許 AWSMigrationHubService 代表客戶呼叫 AWSApplicationDiscoveryService。

`AWSMigrationHubDiscoveryAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMigrationHubDiscoveryAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 8 月 14 日 13：30 UTC
- 編輯時間：2020 年 8 月 6 日 17：34 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMigrationHubDMSAccess

描述： Database Migration Service 在客戶帳戶中擔任角色以呼叫 Migration Hub 的政策

AWSMigrationHubDMSAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSMigrationHubDMSAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 8 月 14 日 14：00 UTC
- 編輯時間：2019 年 10 月 7 日 17：51 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMigrationHubFullAccess

描述：提供客戶 Migration Hub Service 存取權的受管政策

`AWSMigrationHubFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMigrationHubFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 8 月 14 日 14：02 UTC

- **編輯時間**：2019 年 6 月 19 日 21：14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMigrationHubOrchestratorConsoleFullAccess

描述：提供對 AWS Migration Hub、 AWS Application Discovery Service、Amazon Simple Storage Service 和 AWS Secrets Manager 的有限存取權。此政策也會授予 AWS Migration Hub Orchestrator 服務的完整存取權。

AWSMigrationHubOrchestratorConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSMigrationHubOrchestratorConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 4 月 20 日 02：26 UTC
- 編輯時間：2023 年 12 月 5 日 17：34 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHO",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
```

```
    {
      "Sid" : "S3MHO",
      "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*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMigrationHubOrchestratorInstanceRolePolicy

描述：此政策需要為 SAP 和 MGN 遷移執行個體連接，以便我們的服務透過從 S3 下載指令碼並在 EC2 執行個體內擷取秘密值來協調執行個體。

AWSMigrationHubOrchestratorInstanceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSMigrationHubOrchestratorInstanceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 4 月 20 日 02：43 UTC
- 編輯時間：2022 年 4 月 20 日 02：43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMigrationHubOrchestratorPlugin

描述：提供對 AWS Migration Hub Orchestrator 的 Amazon Simple Storage Service、 AWS Secrets Manager 和外掛程式相關動作的有限存取權。

AWSMigrationHubOrchestratorPlugin 是 AWS 受管政策。

使用此政策

您可以將 AWSMigrationHubOrchestratorPlugin 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 4 月 20 日，UTC 02：25
- 編輯時間：2022 年 4 月 20 日 02：25 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMigrationHubOrchestratorServiceRolePolicy

描述：提供 Migration Hub Orchestrator 遷移和現代化現場部署工作負載所需的許可

`AWSMigrationHubOrchestratorServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 4 月 20 日 02：24 UTC
- 編輯時間：2024 年 3 月 4 日 18：25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

描述：授予 AWS Migration Hub Refactor Spaces 和其他 AWS 相關服務的完整存取權，但使用沒有網路橋接的環境時不需要 AWS Transit Gateway 和 EC2 安全群組。此政策也排除 AWS Lambda 和 AWS Resource Access Manager 所需的許可，因為它們可以根據標籤縮小範圍。

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 4 月 3 日 20：09 UTC
- 編輯時間：2024 年 4 月 11 日 18：16 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsDelete",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

描述：在傳遞至 SSM Automation 文件 AWSRefactorSpaces-CreateResources 的 IAM 服務角色中使用 ，以授予執行自動化所需的許可。政策會授予 EC2 標籤的讀取/寫入存取權，以追蹤自動化進度。啟用重構空間環境的網路橋接器時，自動化也會將環境的安全群組新增至 EC2 執行個體，以允許來自環境中其他重構空間服務的流量。此政策也會授予 Application Migration Service 啟動後動作 SSM 參數的存取權。

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 8 月 10 日 15：08 UTC
- 編輯時間：2023 年 8 月 10 日 15：08 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMigrationHubRefactorSpacesFullAccess

描述：授予對 AWS MigrationHub Refactor Spaces、 AWS MigrationHub Refactor Spaces 主控台功能和其他相關 AWS 服務的完整存取權， AWS Lambda 和 AWS Resource Access Manager 所需的許可除外，因為這些功能可以根據標籤縮小範圍。

`AWSMigrationHubRefactorSpacesFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMigrationHubRefactorSpacesFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 11 月 29 日 07：12 UTC
- 編輯時間：2024 年 4 月 11 日 17：45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RequestTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "ResourceTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2NetworkingModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTransitGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
```

```
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
```

```
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMigrationHubRefactorSpacesServiceRolePolicy

描述：提供對 AWS Migration Hub Refactor Spaces 管理或使用 AWS 的資源的存取權。

`AWSMigrationHubRefactorSpacesServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 29 日 06：50 UTC
- 編輯時間：2023 年 7 月 20 日 15：57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSMigrationHubSMSAccess

描述： Server Migration Service 在客戶帳戶中擔任角色以呼叫 Migration Hub 的政策

AWSMigrationHubSMSAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSMigrationHubSMSAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 8 月 14 日 13：57 UTC
- 編輯時間：2019 年 10 月 7 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMigrationHubStrategyCollector

描述：授予許可，以允許與 AWS Migration Hub Strategy Recommendations 服務通訊、讀取/寫入與服務相關的 S3 儲存貯體的存取權、上傳日誌和指標的 Amazon API Gateway 存取權 AWS、擷取登入資料的 AWS Secrets Manager 存取權，以及任何相關服務。

`AWSMigrationHubStrategyCollector` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMigrationHubStrategyCollector` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 10 月 19 日，UTC 20：15
- 編輯時間：2024 年 4 月 1 日 16：21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
```

```
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowS3ListBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowMetricsAndLogs",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:PutMetricData",
        "application-transformation:PutLogData",
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MHSRAllowExecuteAPI",
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
```

```
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
    },
    {
      "Sid" : "MHSRAllowCollectorAPI",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:RegisterCollector",
        "migrationhub-strategy:GetAntiPattern",
        "migrationhub-strategy:GetMessage",
        "migrationhub-strategy:SendMessage",
        "migrationhub-strategy:ListAntiPatterns",
        "migrationhub-strategy:ListJarArtifacts",
        "migrationhub-strategy:UpdateCollectorConfiguration",
        "migrationhub-strategy:PutLogData",
        "migrationhub-strategy:PutMetricData"
      ],
      "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
    },
    {
      "Sid" : "MHSRAllowSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMigrationHubStrategyConsoleFullAccess

描述：授予 AWS Migration Hub Strategy Recommendations 服務的完整存取權，以及透過 存取相關 AWS 服務 AWS 管理主控台。

AWSMigrationHubStrategyConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSMigrationHubStrategyConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 10 月 19 日，UTC 20：13
- 編輯時間：2022 年 11 月 9 日 00：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMigrationHubStrategyServiceRolePolicy

描述：啟用存取 AWS Migration Hub Strategy Recommendations 服務使用或管理 AWS 的資源。

`AWSMigrationHubStrategyServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 10 月 19 日，UTC 20：02
- 編輯時間：2021 年 10 月 19 日，UTC 20：02

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "permissionsForAds",
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "permissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
```

```
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMobileHub_FullAccess

描述：此政策可以連接到任何使用者、角色或群組，以授予使用者在 AWS Mobile Hub 中建立、刪除和修改專案（及其相關 AWS 資源）的許可。這也包含為每個 Mobile Hub 專案產生和下載範例行動應用程式原始程式碼的許可。

`AWSMobileHub_FullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMobileHub_FullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 1 月 5 日 19：56 UTC
- 編輯時間：2019 年 12 月 19 日，UTC 23：15
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

政策版本

政策版本： v14（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSMobileHub_ReadOnly

描述：此政策可以連接到任何使用者、角色或群組，以授予使用者在 AWS Mobile Hub 中列出和檢視專案的許可。這也包含為每個 Mobile Hub 專案產生和下載範例行動應用程式原始程式碼的許可。它不允許使用者修改任何 Mobile Hub 專案的任何組態。

`AWSMobileHub_ReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMobileHub_ReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 1 月 5 日 19：55 UTC
- 編輯時間：2018 年 7 月 23 日，UTC 21：59
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSMSKReplicatorExecutionRole

描述：授予 Amazon MSK Replicator 在 MSK 叢集之間複寫資料的許可。

`AWSMSKReplicatorExecutionRole` 是 AWS 受管政策。

使用此政策

您可以將 `AWSMSKReplicatorExecutionRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 12 月 6 日 00：07 UTC
- 編輯時間：2024 年 3 月 25 日 21：36 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:WriteDataIdempotently"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:cluster/*"
      ]
    },
```

```
    {
      "Sid" : "TopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:AlterCluster"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:topic/*/*"
      ]
    },
    {
      "Sid" : "GroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:group/*/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSNATGatewayServiceRolePolicy

描述：提供管理 VPC 資源的許可，以設定和管理 NAT 閘道。

AWSNATGatewayServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 11 月 14 日 17：19 UTC
- 編輯時間：2025 年 11 月 14 日 17：19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNATGatewayServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSNetworkFirewallFullAccess

描述：授予 AWS Network Firewall 服務的完整存取權，包括建立、設定、管理和刪除防火牆資源、政策和規則群組的許可。此外，還包含修改 VPC 端點、S3 儲存貯體政策、CloudWatch Logs 組態，以及為 Network Firewall 和日誌交付服務建立服務連結角色的許可

`AWSNetworkFirewallFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSNetworkFirewallFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 6 月 10 日 21：52 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:CreateRuleGroup",
        "network-firewall:CreateTLSInspectionConfiguration",
        "network-firewall:DeleteFirewall",
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DeleteRuleGroup",
        "network-firewall:DeleteTLSInspectionConfiguration",
        "network-firewall:DisassociateSubnets",
        "network-firewall:PutResourcePolicy",
        "network-firewall:StartAnalysisReport",
        "network-firewall:StartFlowCapture",
        "network-firewall:StartFlowFlush",
        "network-firewall:UpdateFirewallAnalysisSettings",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallDescription",
        "network-firewall:UpdateFirewallEncryptionConfiguration",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateLoggingConfiguration",
```

```
        "network-firewall:UpdateRuleGroup",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:UpdateTLSInspectionConfiguration"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*"
      ]
    },
    {
      "Sid" : "NetworkFirewallEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallDeleteVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "NetworkFirewallLogging",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallLoggingCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallLoggingS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLoggingFirehose",
      "Effect" : "Allow",
      "Action" : "firehose:TagDeliveryStream",
      "Resource" : "arn:aws:firehose:*:*:*"
    },
```

```
    {
      "Sid" : "NetworkFirewallSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/network-firewall.amazonaws.com/
AWSServiceRoleForNetworkFirewall"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network-firewall.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSNetworkFirewallReadOnlyAccess

描述：透過 、 CLI 和 SDK AWS 管理主控台提供 AWS Network Firewall 資源的唯讀存取權。 SDKs 此政策允許使用者檢視和監控防火牆組態、政策、規則群組和相關聯的資源，而無需進行變更。

AWSNetworkFirewallReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSNetworkFirewallReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 6 月 10 日 21：52 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkFirewallReadOnlyAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListProxies",
        "network-firewall:ListProxyConfigurations",
        "network-firewall:ListProxyRuleGroups",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListVpcEndpointAssociations",
        "network-firewall:DescribeFirewall",
```

```
        "network-firewall:DescribeFirewallMetadata",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeProxy",
        "network-firewall:DescribeProxyConfiguration",
        "network-firewall:DescribeProxyRule",
        "network-firewall:DescribeProxyRuleGroup",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:DescribeVpcEndpointAssociation",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults"
      ],
      "Resource" : "arn:aws:network-firewall:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSNetworkFirewallServiceRolePolicy

描述：允許 AWSNetworkFirewall 建立和管理防火牆的必要資源。

`AWSNetworkFirewallServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 11 月 17 日 17：17 UTC
- 編輯時間：2023 年 3 月 30 日 17：19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSNetworkManagerCloudWANServiceRolePolicy

描述：允許 NetworkManager 存取與核心網路相關聯的資源

`AWSNetworkManagerCloudWANServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 7 月 12 日 12：17 UTC
- 編輯時間：2022 年 7 月 12 日 12：17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSNetworkManagerFullAccess

描述：透過 提供 Amazon NetworkManager 的完整存取權 AWS 管理主控台。

`AWSNetworkManagerFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSNetworkManagerFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 17：37 UTC
- 編輯時間：2019 年 12 月 3 日 17：37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSNetworkManagerReadOnlyAccess

描述：透過 提供 Amazon NetworkManager 的唯讀存取權 AWS 管理主控台。

AWSNetworkManagerReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSNetworkManagerReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 3 日 17：35 UTC
- 編輯時間：2019 年 12 月 3 日 17：35 UTC
- ARN: arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSNetworkManagerServiceRolePolicy

描述：允許 NetworkManager 存取與 Global Networks 相關聯的資源

AWSNetworkManagerServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 12 月 3 日 14：03 UTC
- 編輯時間：2022 年 7 月 27 日 19：41 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeLocations",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpcs",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeRegions",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSObservabilityAdminLogsCentralizationServiceRolePolicy

描述：CloudWatch Logs 集中化的服務連結角色許可

AWSObservabilityAdminLogsCentralizationServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 9 月 15 日 14：34 UTC
- 編輯時間：2025 年 9 月 15 日 14：34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminLogsCentralizationServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "logs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/LogsManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSObservabilityAdminServiceRolePolicy

描述：提供管理 AWS Config Configuration Recorder、管理 AWS Config Configuration Aggregator、為 Configuration Recorder 功能建立 AWS Config Service Linked Role、使用記錄器組態資料，以及為組織功能讀取 AWS Organizations 資料的存取權。

`AWSObservabilityAdminServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 11 月 27 日 19：36 UTC

- **編輯時間**：2024 年 11 月 27 日 19：36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "config:PutConfigurationAggregator",
        "config:DeleteConfigurationAggregator",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
observabilityadmin.amazonaws.com/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "observabilityadmin.amazonaws.com",
            "config.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy

描述：提供存取權，以管理 AWS 資源上的 AWS Config 記錄器資源和遙測設定，包括日誌、指標。

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 8 月 1 日 18：04 UTC
- 編輯時間：2026 年 3 月 11 日 22：27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TelemetryOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeFlowLogs",
        "ec2:DescribeVpcs",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:ListLogGroups",
        "ec2:MonitorInstances",
        "logs:DescribeDeliverySources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "TagOperationForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateFlowLogs"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TagOperationForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCFlowLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-flow-log/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteFlowLogs",
        "logs:CreateDelivery",
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliverySource",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSApiLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/api" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/audit" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuthenticatorLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "Bool" : {
          "eks:loggingType/authenticator" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSControllerManagerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/controllerManager" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSSchedulerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/scheduler" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLoggingConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
```

```
      "Resource" : "arn:aws:wafv2:*:*:regional/webacl/*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:logs:*:*:log-group:*"
        },
        "StringEquals" : {
          "wafv2:LogScope" : "CloudwatchTelemetryRuleManaged",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForBedrock",
```

```
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForCloudTrailLogs",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/cloudwatch/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForManagedLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/cloudtrail",
        "arn:aws:logs:*:*:log-group:aws/cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "Route53QueryLoggingListOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigCreation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:CreateResolverQueryLogConfig",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:resolver-query-log-config/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "Route53QueryLoggingConfigAssociation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateResolverQueryLogConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/route53resolver.amazonaws.com/
AWSServiceRoleForRoute53Resolver",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "route53resolver.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMOperationsForConfigServiceLinkedRecorder",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ManagementOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin_TelemetryEnablement/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "telemetry-enablement.observabilityadmin.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSOrganizationsFullAccess

描述：提供 AWS Organizations 的完整存取權。

`AWSOrganizationsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSOrganizationsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 6 日 20：31 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "account:PutAccountName",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSOrganizationsReadOnlyAccess

描述：提供 AWS Organizations 的唯讀存取權。

`AWSOrganizationsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSOrganizationsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 11 月 6 日 20：32 UTC
- 編輯時間：2024 年 6 月 7 日 21：32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSOrganizationsServiceTrustPolicy

描述：允許 AWS Organizations 與其他已核准 AWS 服務 的 共用信任以簡化客戶組態的政策。

AWSOrganizationsServiceTrustPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 10 日 23：04 UTC
- 編輯時間：2026 年 3 月 5 日 19：12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    },
    {
      "Sid" : "ListRolesSLR",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSOutpostsAuthorizeServerPolicy

描述：此政策授予許可，允許您在內部部署網路上安裝 Outpost 伺服器。

AWSOutpostsAuthorizeServerPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSOutpostsAuthorizeServerPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 1 月 4 日 19：23 UTC
- 編輯時間：2023 年 1 月 4 日 19：23 UTC
- ARN: arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSOutpostsServiceRolePolicy

描述：服務連結角色政策，以啟用存取 Outposts AWS 管理 AWS 的資源

AWSOutpostsServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 11 月 9 日，UTC 22：55
- 編輯時間：2025 年 4 月 17 日 17：37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateConnectivityServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfacePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
```

```
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfaceTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSPanoramaApplianceRolePolicy

描述：允許 AWS Panorama 設備上的 AWS IoT 軟體將日誌上傳至 Amazon CloudWatch。

`AWSPanoramaApplianceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSPanoramaApplianceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 12 月 1 日 13：13 UTC
- 編輯時間：2020 年 12 月 1 日 13：13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPanoramaApplianceServiceRolePolicy

描述：允許 AWS Panorama 設備將日誌上傳至 Amazon CloudWatch，並從建立用於 AWS Panorama 的 Amazon S3 存取點取得物件。

AWSPanoramaApplianceServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSPanoramaApplianceServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 10 月 20 日 12：14 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSPanoramaFullAccess

描述：提供 AWS Panorama 的完整存取權

AWSPanoramaFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSPanoramaFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 1 日 13：12 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSPanoramaFullAccess

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "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"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPanoramaGreengrassGroupRolePolicy

描述：允許 AWS Panorama 設備上的 AWS Lambda 函數管理 Panorama 中的資源、將日誌和指標上傳至 Amazon CloudWatch，以及管理建立用於 Panorama 的儲存貯體中的物件。

`AWSPanoramaGreengrassGroupRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSPanoramaGreengrassGroupRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 12 月 1 日 13：10 UTC
- 編輯時間：2021 年 1 月 6 日 19：30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSPanoramaSageMakerRolePolicy

描述：允許 Amazon SageMaker 管理建立用於 AWS Panorama 的儲存貯體中的物件。

AWSPanoramaSageMakerRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSPanoramaSageMakerRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 12 月 1 日 13：13 UTC
- 編輯時間：2020 年 12 月 1 日 13：13 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSPanoramaServiceLinkedRolePolicy

描述：允許 AWS Panorama 管理 AWS IoT、 AWS Secrets Manager 和 AWS Panorama 中的資源。

AWSPanoramaServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 10 月 20 日 12：12 UTC
- 編輯時間：2021 年 10 月 20 日 12：12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSPanoramaServiceRolePolicy

描述：允許 AWS Panorama 管理 Amazon S3、 AWS IoT、 AWS IoT GreenGrass、 AWS Lambda、Amazon SageMaker 和 Amazon CloudWatch Logs 中的資源，並將服務角色傳遞至 AWS IoT、 AWS IoT GreenGrass 和 Amazon SageMaker。

`AWSPanoramaServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSPanoramaServiceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 12 月 1 日 13：14 UTC
- 編輯時間：2020 年 12 月 1 日 13：14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*",
        "panorama:Get*"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaSageMakerRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaSageMakerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
```

```
        "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassIoTRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PanoramaGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
```

```
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteResourceDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
```

```
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:StopCompilationJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/panorama*",
        "arn:aws:sagemaker:*:*:compilation-job/panorama*"
      ]
    },
    {
```

```
      "Sid" : "PanoramaSageMakerListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCompilationJobs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "PanoramaCWLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:CreateRoleAlias"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*",
        "arn:aws:iot:*:*:rolealias/panorama*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSPartnerCentralChannelHandshakeApprovalManagement

描述：提供頻道交握核准管理活動的必要存取權。

AWSPartnerCentralChannelHandshakeApprovalManagement 是 AWS 受管政策。

使用此政策

您可以將 AWSPartnerCentralChannelHandshakeApprovalManagement 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 11 月 19 日 16：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralChannelHandshakeApprovalManagement

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelHandshakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListChannelHandshakes",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPartnerCentralChannelManagement

描述：提供頻道管理活動的必要存取權。

AWSPartnerCentralChannelManagement 是 AWS 受管政策。

使用此政策

您可以將 AWSPartnerCentralChannelManagement 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 19 日 16：34 UTC
- 編輯時間：2026 年 2 月 14 日 00：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralChannelManagement

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateProgramManagementAccount",
        "partnercentral:UpdateProgramManagementAccount",
        "partnercentral:DeleteProgramManagementAccount",
        "partnercentral:ListProgramManagementAccounts",
        "partnercentral:GetProgramManagementAccount",
        "partnercentral:CreateRelationship",
        "partnercentral:UpdateRelationship",
        "partnercentral:DeleteRelationship",
        "partnercentral:GetRelationship",
        "partnercentral:ListRelationships",
        "partnercentral:CreateChannelHandshake",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake",
        "partnercentral:CancelChannelHandshake",
        "partnercentral:ListChannelHandshakes"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/program-management-account/*",
        "arn:aws:partnercentral:*:*:catalog/*/channel-handshake/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "ChannelUser"
        }
      }
    },
```

```
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Resell_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSPartnerCentralFullAccess

描述：提供 AWS Partner Central 和相關 的完整存取權 AWS 服務。

`AWSPartnerCentralFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSPartnerCentralFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 18 日 23：33 UTC
- 編輯時間：2026 年 3 月 12 日 17：12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralFullAccess`

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "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" : "*"
    },
    {
      "Sid" : "AWSPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
```

```
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "SupportAccess",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "support:AddAttachmentsToSet",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListEntitiesAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
```

```
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSPartnerCentralMarketingManagement

描述：提供行銷活動的必要存取權。

AWSPartnerCentralMarketingManagement 是 AWS 受管政策。

使用此政策

您可以將 AWSPartnerCentralMarketingManagement 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 12 月 1 日 00：34 UTC
- 編輯時間：2026 年 2 月 14 日 00：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralMarketingManagement

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "MarketingStaff"
        }
      }
    },
    {
      "Sid" : "PartnerDiscoveryAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:SearchPartnerProfiles",
        "partnercentral:GetPartnerProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartProfileUpdateTask",
        "partnercentral:GetProfileUpdateTask",
        "partnercentral:CancelProfileUpdateTask",
```

```
        "partnercentral:PutProfileVisibility",
        "partnercentral:GetProfileVisibility"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
```

```
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/MarketingCampaign_V1/
Dashboard/*"
      ]
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPartnerCentralOpportunityManagement

描述：提供機會管理活動的必要存取權。

AWSPartnerCentralOpportunityManagement 是 AWS 受管政策。

使用此政策

您可以將 AWSPartnerCentralOpportunityManagement 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 14 日 19：09 UTC
- 編輯時間：2026 年 3 月 12 日 17：12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralOpportunityManagement`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpportunityManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:AcceptEngagementInvitation",
        "partnercentral:AssignOpportunity",
        "partnercentral:AssociateOpportunity",
        "partnercentral:CreateEngagement",
        "partnercentral:CreateEngagementContext",
        "partnercentral:CreateEngagementInvitation",
        "partnercentral:CreateOpportunity",
        "partnercentral:CreateResourceSnapshot",
        "partnercentral:CreateResourceSnapshotJob",
        "partnercentral:DeleteResourceSnapshotJob",
        "partnercentral:DisassociateOpportunity",
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetEngagement",
        "partnercentral:GetEngagementInvitation",
        "partnercentral:GetOpportunity",
        "partnercentral:GetResourceSnapshot",
        "partnercentral:GetResourceSnapshotJob",
        "partnercentral:ListEngagementByAcceptingInvitationTasks",
```

```
        "partnercentral:ListEngagementFromOpportunityTasks",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagementMembers",
        "partnercentral:ListEngagementResourceAssociations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListOpportunityFromEngagementTasks",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "partnercentral:ListSolutions",
        "partnercentral:RejectEngagementInvitation",
        "partnercentral:StartEngagementByAcceptingInvitationTask",
        "partnercentral:StartEngagementFromOpportunityTask",
        "partnercentral:StartOpportunityFromEngagementTask",
        "partnercentral:StartResourceSnapshotJob",
        "partnercentral:StopResourceSnapshotJob",
        "partnercentral:SubmitOpportunity",
        "partnercentral:UpdateEngagementContext",
        "partnercentral:UpdateOpportunity"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
```

```
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "AceManager"
        }
      }
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Opportunity_V1/Dashboard/
*",
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Engagement_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "CollaborationChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateCollaborationChannelRequest",
        "partnercentral:ListCollaborationChannels",
        "partnercentral:GetCollaborationChannel",
        "partnercentral:CreateCollaborationChannelMembers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerResourceAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/*/resource-snapshot-job/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonQPartnerAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
```

```
        "q:PassRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPartnerCentralSandboxFullAccess

描述：在沙盒目錄中提供開發人員測試的必要存取權。

AWSPartnerCentralSandboxFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSPartnerCentralSandboxFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 11 月 14 日 19：10 UTC
- 編輯時間：2026 年 3 月 12 日 17：12 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralSandboxFullAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPartnerCentralSandboxAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        }
      }
    },
    {
      "Sid" : "PartnerCentralAgentsSandboxSessionAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        },
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

描述：提供 ResourceSnapshotJob 的存取權，以讀取資源並在目標參與中將其快照。

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 10 日 18：21 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateResourceSnapshot"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*::catalog/AWS/engagement/*",
        "arn:aws:partnercentral:*::catalog/Sandbox/engagement/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetOpportunity"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/AWS/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/Sandbox/opportunity/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSPartnerLedSupportReadOnlyAccess

描述：此政策可用來授予 API 的唯讀存取權，這些 APIs 可以讀取您 中 服務的服務中繼資料 AWS 帳戶。您可以使用此政策，讓合作夥伴領導支援計劃中的合作夥伴能夠存取以下許可詳細資訊區段中指定的服務。

`AWSPartnerLedSupportReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSPartnerLedSupportReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 11 月 22 日 20：06 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerLedSupportReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "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/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "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",
        "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",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
```

```
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupPlans",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeStacks",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
```

```
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listStacks",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypeVersions",
        "cloudformation:listTypes",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
```

```
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "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:listMetricStreams",
        "cloudwatch:listMetrics",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineState",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "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",
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationFormVersions",
        "connect:listEvaluationForms",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
        "connect:listViewVersions",
        "connect:listViews",
        "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:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEndpoints",
        "dms:describeEventCategories",
        "dms:describeEventSubscriptions",
        "dms:describeEvents",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationInstances",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "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",
        "ec2:describeAccountAttributes",
        "ec2:describeAddressTransfers",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "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:describeIdFormat",
        "ec2:describeIdentityIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
```

```
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInstances",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpamScopes",
        "ec2:describeIpams",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLaunchTemplates",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeLocalGateways",
        "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:describeSnapshotTierStatus",
        "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:describeTransitGatewayVpcAttachments",
        "ec2:describeTransitGateways",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumeStatus",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "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: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:getSubnetCidrReservations",
            "ec2:getTransitGatewayMulticastDomainAssociations",
            "ec2:getTransitGatewayPrefixListReferences",
            "ec2:getVerifiedAccessEndpointPolicy",
            "ec2:getVerifiedAccessGroupPolicy",
            "ec2:listImagesInRecycleBin",
            "ec2:listSnapshotsInRecycleBin",
            "ec2:searchLocalGatewayRoutes",
            "ec2:searchTransitGatewayMulticastGroups",
            "ec2:searchTransitGatewayRoutes",
            "ecs:describeCapacityProviders",
            "ecs:describeClusters",
            "ecs:describeContainerInstances",
            "ecs:describeServices",
            "ecs:describeTaskDefinition",
            "ecs:describeTaskSets",
            "ecs:describeTasks",
            "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:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "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:describeServerlessCacheSnapshots",
        "elasticache:describeServerlessCaches",
        "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:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeMountTargets",
        "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",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "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",
            "events:describeApiDestination",
            "events:describeArchive",
            "events:describeConnection",
            "events:describeEndpoint",
            "events:describeEventBus",
            "events:describeEventSource",
            "events:describePartnerEventSource",
            "events:describeReplay",
            "events:describeRule",
            "events:listApiDestinations",
            "events:listArchives",
            "events:listConnections",
            "events:listEndpoints",
            "events:listEventBuses",
            "events:listEventSources",
            "events:listPartnerEventSourceAccounts",
            "events:listPartnerEventSources",
            "events:listReplays",
            "events:listRuleNamesByTarget",
            "events:listRules",
            "events:listTargetsByRule",
            "events:testEventPattern",
            "fsx:describeBackups",
            "fsx:describeDataRepositoryAssociations",
            "fsx:describeDataRepositoryTasks",
            "fsx:describeFileCaches",
            "fsx:describeFileSystems",
            "fsx:describeSnapshots",
            "fsx:describeStorageVirtualMachines",
            "fsx:describeVolumes",
            "fsx:listTagsForResource",
            "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:getDataQualityResult",
            "glue:getDataQualityRuleRecommendationRun",
            "glue:getDataQualityRuleset",
            "glue:getDataQualityRulesetEvaluationRun",
            "glue:getDatabase",
            "glue:getDatabases",
            "glue:getDataflowGraph",
            "glue:getDevEndpoint",
            "glue:getDevEndpoints",
            "glue:getJob",
            "glue:getJobRun",
            "glue:getJobRuns",
            "glue:getJobs",
            "glue:getMLTaskRun",
            "glue:getMLTaskRuns",
            "glue:getMLTransform",
            "glue:getMLTransforms",
            "glue:getMapping",
            "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:getTableVersions",
            "glue:getTables",
            "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:listSchemaVersions",
            "glue:listSchemas",
            "glue:listSessions",
            "glue:listStatements",
            "glue:querySchemaVersionMetadata",
            "guardduty:getFindings",
            "guardduty:listDetectors",
            "guardduty:listFindings",
            "guardduty:listIPSets",
            "guardduty:listThreatIntelSets",
            "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:getSSHPublicKey",
            "iam:getServerCertificate",
            "iam:getServiceLinkedRoleDeletionStatus",
            "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:listSSHPublicKeys",
            "iam:listServerCertificates",
            "iam:listSigningCertificates",
            "iam:listUserPolicies",
            "iam:listUsers",
            "iam:listVirtualMFADevices",
            "kafka:describeCluster",
            "kafka:describeClusterOperation",
            "kafka:describeClusterOperationV2",
            "kafka:describeClusterV2",
            "kafka:describeConfiguration",
            "kafka:describeConfigurationRevision",
            "kafka:describeReplicator",
            "kafka:describeVpcConnection",
            "kafka:getBootstrapBrokers",
            "kafka:getClusterPolicy",
            "kafka:listClientVpcConnections",
            "kafka:listClusterOperations",
            "kafka:listClusterOperationsV2",
            "kafka:listClusters",
            "kafka:listClustersV2",
            "kafka:listConfigurationRevisions",
            "kafka:listConfigurations",
            "kafka:listNodes",
            "kafka:listReplicators",
```

```
            "kafka:listScramSecrets",
            "kafka:listVpcConnections",
            "kafkaconnect:describeConnector",
            "kafkaconnect:describeCustomPlugin",
            "kafkaconnect:describeWorkerConfiguration",
            "kafkaconnect:listConnectors",
            "kafkaconnect:listCustomPlugins",
            "kafkaconnect:listWorkerConfigurations",
            "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:listFunctionUrlConfigs",
            "lambda:listFunctions",
            "lambda:listFunctionsByCodeSigningConfig",
            "lambda:listLayerVersions",
            "lambda:listLayers",
            "lambda:listProvisionedConcurrencyConfigs",
            "lambda:listVersionsByFunction",
            "logs:describeExportTasks",
            "logs:describeLogGroups",
            "logs:describeLogStreams",
            "logs:describeMetricFilters",
            "logs:describeSubscriptionFilters",
            "medialive:listChannels",
            "medialive:listInputSecurityGroups",
            "medialive:listInputs",
            "mobiletargeting:getAdmChannel",
            "mobiletargeting:getApnsChannel",
```

```
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "pipes:listPipes",
        "polly:describeVoices",
        "polly:listLexicons",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "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:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboardVersions",
        "quicksight:listDashboards",
        "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:listTemplateVersions",
        "quicksight:listTemplates",
        "quicksight:listThemeAliases",
        "quicksight:listThemeVersions",
        "quicksight:listThemes",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
```

```
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "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:describeEventSubscriptions",
        "rds:describeEvents",
        "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-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",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
        "redshift:describeClusters",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
        "redshift:describeEventSubscriptions",
        "redshift:describeEvents",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "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",
        "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:listMultiRegionAccessPoints",
        "s3:listMultipartUploadParts",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
```

```
        "s3express:listAllMyDirectoryBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
```

```
            "sagemaker:describeNotebookInstanceLifecycleConfig",
            "sagemaker:describePipeline",
            "sagemaker:describePipelineDefinitionForExecution",
            "sagemaker:describePipelineExecution",
            "sagemaker:describeProcessingJob",
            "sagemaker:describeProject",
            "sagemaker:describeSpace",
            "sagemaker:describeStudioLifecycleConfig",
            "sagemaker:describeSubscribedWorkteam",
            "sagemaker:describeTrainingJob",
            "sagemaker:describeTransformJob",
            "sagemaker:describeTrial",
            "sagemaker:describeTrialComponent",
            "sagemaker:describeUserProfile",
            "sagemaker:describeWorkforce",
            "sagemaker:describeWorkteam",
            "sagemaker:getDeviceFleetReport",
            "sagemaker:getModelPackageGroupPolicy",
            "sagemaker:getSagemakerServicecatalogPortfolioStatus",
            "sagemaker:listActions",
            "sagemaker:listAlgorithms",
            "sagemaker:listAliases",
            "sagemaker:listAppImageConfigs",
            "sagemaker:listApps",
            "sagemaker:listArtifacts",
            "sagemaker:listAssociations",
            "sagemaker:listAutoMLJobs",
            "sagemaker:listCandidatesForAutoMLJob",
            "sagemaker:listClusterNodes",
            "sagemaker:listClusters",
            "sagemaker:listCodeRepositories",
            "sagemaker:listCompilationJobs",
            "sagemaker:listContexts",
            "sagemaker:listDataQualityJobDefinitions",
            "sagemaker:listDeviceFleets",
            "sagemaker:listDevices",
            "sagemaker:listDomains",
            "sagemaker:listEdgeDeploymentPlans",
            "sagemaker:listEdgePackagingJobs",
            "sagemaker:listEndpointConfigs",
            "sagemaker:listEndpoints",
            "sagemaker:listExperiments",
            "sagemaker:listFeatureGroups",
            "sagemaker:listFlowDefinitions",
```

```
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubContents",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImageVersions",
        "sagemaker:listImages",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelCards",
        "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:listPipelineExecutionSteps",
        "sagemaker:listPipelineExecutions",
        "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",
            "scheduler:listScheduleGroups",
            "scheduler:listSchedules",
            "servicequotas:listAWSDefaultServiceQuotas",
            "servicequotas:listServiceQuotas",
            "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",
            "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",
            "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:listRotationShifts",
            "ssm-contacts:listRotations",
            "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:describeAssociationExecutionTargets",
        "ssm:describeAssociationExecutions",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInstancePatches",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeOpsItems",
```

```
            "ssm:describeParameters",
            "ssm:describePatchBaselines",
            "ssm:describePatchGroupState",
            "ssm:describePatchGroups",
            "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:listAssociationVersions",
            "ssm:listAssociations",
            "ssm:listCommandInvocations",
            "ssm:listCommands",
            "ssm:listComplianceItems",
            "ssm:listComplianceSummaries",
            "ssm:listDocumentMetadataHistory",
            "ssm:listDocumentVersions",
            "ssm:listDocuments",
            "ssm:listOpsItemEvents",
            "ssm:listOpsItemRelatedItems",
            "ssm:listOpsMetadata",
            "ssm:listResourceComplianceSummaries",
            "ssm:listResourceDataSync",
            "ssm:listTagsForResource",
            "swf:describeActivityType",
            "swf:describeDomain",
            "swf:describeWorkflowExecution",
            "swf:describeWorkflowType",
```

```
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "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:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServiceNetworks",
        "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",
        "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:describeApplicationAssociations",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPCSComputeNodePolicy

描述：准許 AWS PCS 運算節點連線至 AWS PCS 叢集。

AWSPCSComputeNodePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSPCSComputeNodePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 6 月 23 日 18：07 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSPCSComputeNodePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "pcs:RegisterComputeNodeGroupInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPCSServiceRolePolicy

描述：授予 PCS 代表您管理資源的許可。

AWSPCSServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 8 月 27 日 16：01 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSPCSServiceRolePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfacesInSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PermissionsToManagePCSNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "PermissionsToDescribePCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreatePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToManagePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
```

```
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTerminatePCSManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*/AWSPCS*",
        "arn:aws:iam::*:role/AWSPCS*",
        "arn:aws:iam::*:role/aws-pcs/*",
        "arn:aws:iam::*:role/*/aws-pcs/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToControlClusterInstanceAttributes",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "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:resource-groups:*:*:group/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Sid" : "PermissionsToProvisionClusterInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagPCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "CreateFleet",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToPublishMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/PCS"
        }
      }
    },
    {
      "Sid" : "PermissionsToManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:pcs!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "pcs",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPriceListServiceFullAccess

描述：提供 AWS Price List Service 的完整存取權。

AWSPriceListServiceFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSPriceListServiceFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 22 日 00：36 UTC
- 編輯時間：2024 年 7 月 2 日 13：34 UTC
- ARN: arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPrivateCAAuditor

描述：提供稽核人員對 AWS 私有憑證授權單位的存取權

AWSPrivateCAAuditor 是 AWS 受管政策。

使用此政策

您可以將 AWSPrivateCAAuditor 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 2 月 14 日 18：33 UTC
- 編輯時間：2023 年 2 月 14 日 18：33 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAAuditor

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPrivateCAConnectorForKubernetesPolicy

描述：授予適用於 Kubernetes 的 AWS Private CA Connector 的基本許可。

AWSPrivateCAConnectorForKubernetesPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSPrivateCAConnectorForKubernetesPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 5 月 19 日，UTC 19：22
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAConnectorForKubernetesPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSPrivateCAFullAccess

描述：提供 AWS 私有憑證授權機構的完整存取權

AWSPrivateCAFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSPrivateCAFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 2 月 14 日 18：20 UTC
- 編輯時間：2023 年 2 月 14 日 18：20 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPrivateCAPrivilegedUser

描述：提供私有憑證授權單位的特權 AWS 憑證使用者存取權

AWSPrivateCAPrivilegedUser 是 AWS 受管政策。

使用此政策

您可以將 AWSPrivateCAPrivilegedUser 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 2 月 14 日 18：26 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSPrivateCAReadOnly

描述：提供 AWS 私有憑證授權單位的唯讀存取權

AWSPrivateCAReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSPrivateCAReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 2 月 14 日 18：30 UTC
- 編輯時間：2023 年 2 月 14 日 18：30 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAReadOnly

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPrivateCAUser

描述：提供憑證使用者對 AWS 私有憑證授權單位的存取權

AWSPrivateCAUser 是 AWS 受管政策。

使用此政策

您可以將 AWSPrivateCAUser 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 2 月 14 日 18：16 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateCAUser

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPrivateMarketplaceAdminFullAccess

描述：提供 AWS 私有 Marketplace 所有管理動作的完整存取權。

`AWSPrivateMarketplaceAdminFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSPrivateMarketplaceAdminFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 11 月 27 日 16：32 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceGetRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*AWSServiceRoleForPrivateMarketplaceAdmin"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/private-
marketplace.marketplace.amazonaws.com/AWSServiceRoleForPrivateMarketplaceAdmin"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:AWSServiceName" : "private-marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceManageDelegatedAdministratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceEnableServiceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "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" : "*"
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPrivateMarketplaceRequests

描述：提供在 AWS Private Marketplace 中建立請求的存取權。

`AWSPrivateMarketplaceRequests` 是 AWS 受管政策。

使用此政策

您可以將 `AWSPrivateMarketplaceRequests` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 10 月 28 日 21：44 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Sid" : "LegacyPrivateMarketplaceRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceManageRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateProductProcurementRequest",
            "CancelProductProcurementRequest"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceReadRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceListRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
```

```
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceReadChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceTaggingRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPrivateNetworksServiceRolePolicy

描述：允許 AWS Private Networks Service 代表客戶管理資源。

`AWSPrivateNetworksServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 12 月 16 日 23：17 UTC
- 編輯時間：2021 年 12 月 16 日 23：17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSProtonCodeBuildProvisioningBasicAccess

描述： Permissions CodeBuild 需要執行 AWS Proton CodeBuild Provisioning 的組建。

AWSProtonCodeBuildProvisioningBasicAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSProtonCodeBuildProvisioningBasicAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 9 日 21：04 UTC
- 編輯時間：2022 年 11 月 9 日 21：04 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSProtonCodeBuildProvisioningServiceRolePolicy

描述：允許 AWS Proton 代表您使用 CodeBuild 和其他 AWS 服務來管理 Proton 資源佈建。

`AWSProtonCodeBuildProvisioningServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 9 日 21：32 UTC
- 編輯時間：2023 年 5 月 17 日 16：11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSProtonDeveloperAccess

描述：提供 AWS Proton APIs和管理主控台的存取權，但不允許管理 Proton 範本或環境。

AWSProtonDeveloperAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSProtonDeveloperAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 2 月 17 日 19：02 UTC
- 編輯時間：2024 年 6 月 6 日 18：26 UTC
- ARN: arn:aws:iam::aws:policy/AWSProtonDeveloperAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "codestar-connections:UseConnection",
        "proton:CancelServiceInstanceDeployment",
        "proton:CancelServicePipelineDeployment",
        "proton:CreateService",
        "proton:DeleteService",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
```

```
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSProtonFullAccess

描述：提供 AWS Proton APIs和管理主控台的完整存取權。除了這些許可之外，還需要存取 Amazon S3 才能從 S3 儲存貯體註冊範本套件，以及存取 Amazon IAM 來建立和管理 Proton 的服務角色。

`AWSProtonFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSProtonFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 2 月 17 日 19：07 UTC
- 編輯時間：2024 年 6 月 6 日 18：29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "PassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sync.proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:PassConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:PassConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSProtonReadOnlyAccess

描述：提供 AWS Proton APIs唯讀存取權。

`AWSProtonReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSProtonReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2021 年 2 月 17 日，UTC 19：09

- **編輯時間**：2022 年 11 月 18 日 18：28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSProtonServiceGitSyncServiceRolePolicy

描述：允許 AWS Proton 將您的服務、環境和元件定義從 git 儲存庫同步到 AWS Proton 的政策。

AWSProtonServiceGitSyncServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 4 月 4 日 15：55 UTC
- 編輯時間：2023 年 4 月 4 日 15：55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSProtonSyncServiceRolePolicy

描述：允許 AWS Proton 將 git 儲存庫內容同步至 Proton 或將 Proton 內容同步至 git 儲存庫的政策。

`AWSProtonSyncServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 23 日 21：14 UTC
- 編輯時間：2024 年 5 月 5 日，UTC 01：49
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
```

```
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSPurchaseOrdersServiceRolePolicy

描述：授予在帳單主控台上檢視和修改採購訂單的許可

AWSPurchaseOrdersServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSPurchaseOrdersServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 5 月 6 日 18：15 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "aws-portal:*Billing",
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceUnits",
        "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSetupCFGCPacksPermissionsBoundary

描述：AWSQuickSetupCFGCPacksPermissionsBoundary 政策會定義 Quick Setup 建立的 IAM 角色中允許的許可清單。快速設定使用此政策建立的角色來部署 AWS Config 一致性套件。

AWSQuickSetupCFGCPacksPermissionsBoundary 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupCFGCPacksPermissionsBoundary 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：52 UTC
- 編輯時間：2024 年 6 月 26 日 09：52 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ]
    },
```

```
    {
      "Sid" : "ConfigurationRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutCPackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack"
      ],
      "Resource" : [
        "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeCPacksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConformancePacksSLRCreatePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EnableExplorerReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceSettingsForExplorerUpdatePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupDeploymentRolePolicy

描述：提供 AWS Systems Manager Quick Setup 部署多種組態類型的許可。這些組態類型會建立 IAM 角色和自動化，透過建議的最佳實務來設定常用的 Amazon Web Services 服務和功能。

AWSQuickSetupDeploymentRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupDeploymentRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：55 UTC

- **編輯時間**：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDeploymentRolePolicy`

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
```

```
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CPacksRead",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePacks",
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OpsPacksManage",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
```

```
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPackInstance-*"
      ]
    },
    {
      "Sid" : "QSDocsRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState"
```

```
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "EventRulesManage",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DescribeRule",
        "events:PutRule",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*QuickSetup-*"
      ]
    },
    {
      "Sid" : "CPacksSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "QSConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRolePass",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
```

```
      "Sid" : "QSConfigRoleBounded",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : [
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGRecordingPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRoleManagedPolicies",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSSystemsManagerEnableConfigRecordingExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy",
```

```
            "arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupDevOpsGuruPermissionsBoundary

描述：AWSQuickSetupDevOpsGuruPermissionsBoundary 政策會定義 Quick Setup 建立的 IAM 角色中允許的許可清單。快速設定使用此政策建立的角色來啟用和設定 Amazon DevOps Guru。此政策也提供啟用 Systems Manager Explorer 的許可。

AWSQuickSetupDevOpsGuruPermissionsBoundary 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupDevOpsGuruPermissionsBoundary 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2024 年 6 月 26 日 09：44 UTC
- 編輯時間：2024 年 6 月 26 日 09：44 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateDevOpsGuruSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudformationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruNotificationChannelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:AddNotificationChannel"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:DevOpsGuru-Default-Topic",
        "arn:aws:devops-guru:*:*:/channels"
      ]
    },
    {
      "Sid" : "DevOpsGuruConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:UpdateResourceCollection",
        "devops-guru:UpdateServiceIntegration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DevOpsGuruDefaultSNSTopicConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:RemovePermission"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOpsGuru-Default-Topic"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSetupDistributorPermissionsBoundary

描述：QuickSetup 會建立 IAM 角色，使其能夠代表您設定 Systems Manager Distributor 功能，並在建立此類角色時使用此政策來定義其許可界限。

`AWSQuickSetupDistributorPermissionsBoundary` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSetupDistributorPermissionsBoundary` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：50 UTC
- 編輯時間：2024 年 6 月 26 日 09：50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DistributorAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ]
    },
    {
      "Sid" : "DistributorAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
```

```
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
```

```
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-ConfigureAWSPackage*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
```

```
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupEnableAREXExecutionPolicy

描述：此政策授予許可，允許 Systems Manager 執行 AWSQuickSetupType-EnableAREX Automation Runbook，這可讓 AWS Resource Explorer 與 Systems Manager 搭配使用。

`AWSQuickSetupEnableAREXExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupEnableAREXExecutionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 15 日 22：45 UTC
- 編輯時間：2024 年 11 月 15 日 22：45 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupEnableAREXExecutionPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadActions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowUpdateExistingIndexAndAssociateDefaultView",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:AssociateDefaultView"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateViewAndIndex",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:TagResource"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*:*:view/all-resources/*",
        "arn:aws:resource-explorer-2:*:*:index/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Type" : "QuickSetup",
          "aws:ResourceTag/Type" : "QuickSetup"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Type"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSetupEnableDHMCExecutionPolicy

描述：此政策授予許可，允許主體執行 AWSQuickSetupType-EnableDHMC Automation Runbook，這會啟用預設主機管理組態。

AWSQuickSetupEnableDHMCExecutionPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupEnableDHMCExecutionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 15 日 21：27 UTC
- 編輯時間：2024 年 11 月 15 日 21：27 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupEnableDHMCExecutionPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AmazonSSMManagedEC2InstanceDefaultPolicy"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/default-ec2-
instance-management-role"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupJITNADeploymentRolePolicy

描述：此政策允許快速設定部署設定just-in-time節點存取所需的組態類型。

AWSQuickSetupJITNADeploymentRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupJITNADeploymentRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 4 月 17 日 09：07 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupJITNADeploymentRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-JITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
```

```
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
        "arn:aws:ssm:*::document/AWSQuickSetupType-
PropagateJustInTimeNodeAccessPolicies",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
```

```
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::*:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-JITNA"
        },
        "ArnLike" : {
```

```
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSetupManagedInstanceProfileExecutionPolicy

描述：此政策授予管理許可，允許 Systems Manager 為快速設定功能建立預設 IAM 執行個體描述檔，並將其連接到尚未連接執行個體的 Amazon EC2 執行個體。 描述檔。

`AWSQuickSetupManagedInstanceProfileExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSetupManagedInstanceProfileExecutionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 15 日 21：51 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManagedInstanceProfileExecutionPolicy`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfilesForRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachAmazonSSMManagedInstanceCore",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation",
```

```
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess",
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "InstanceProfileAssociationEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutomationsStartWithTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ],
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AutomationsGetPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:GetAutomationExecution",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "GetQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    },
    {
      "Sid" : "PassQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
```

```
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSetupManageJITNAResourcesExecutionPolicy

描述：此政策提供許可，以啟用 Systems Manager just-in-time節點存取。

AWSQuickSetupManageJITNAResourcesExecutionPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupManageJITNAResourcesExecutionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 4 月 17 日 21：37 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateJustInTimeAccessServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/justintimeaccess.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerJustInTimeAccess"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "justintimeaccess.ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSystemsManagerNotificationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/notifications.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerNotifications"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "notifications.ssm.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::*:policy/
AWSSystemsManagerJustInTimeAccessTokenPolicy"
        }
      }
    },
    {
      "Sid" : "IAMRoleManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceSettingsManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/just-in-time-access/identity-provider"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupPatchPolicyBaselineAccess

描述：提供唯讀許可，以使用快速設定存取目前 AWS 帳戶 或組織中管理員所設定的修補程式基準。

AWSQuickSetupPatchPolicyBaselineAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupPatchPolicyBaselineAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：38 UTC
- 編輯時間：2024 年 6 月 26 日 09：38 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3SameAccountReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3OrganizationReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalOrgID" : [
            "${aws:ResourceOrgID}"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupPatchPolicyDeploymentRolePolicy

描述：提供許可，允許快速設定建立與修補程式政策組態相關聯的資源。

AWSQuickSetupPatchPolicyDeploymentRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupPatchPolicyDeploymentRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：57 UTC
- 編輯時間：2024 年 6 月 26 日 09：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3BucketsList",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AccessLogsBucketManage",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:Put*",
        "s3:Get*",
        "s3:List*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:s3:::aws-quicksetup-patchpolicy-access-log-*"
      ]
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:UpdateFunction*",
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:DeleteFunction",
        "lambda:InvokeFunction",
        "lambda:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
```

```
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ]
    },
    {
      "Sid" : "LogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogGroupsManage",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "logs:DeleteLogGroup",
        "logs:ListTagsForResource",
        "logs:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
```

```
        "ssm:DescribeDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*"
      ]
    },
    {
      "Sid" : "QSDocsGet",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline"
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "ConfigRolePassToSSM",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConfigRolePassToLambda",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "ConfigRoleBoundedManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
```

```
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AWSQuickSetupPatchPolicyPermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupPatchPolicyPermissionsBoundary

描述：QuickSetup 會建立 IAM 角色，使其能夠代表您設定 Systems Manager Patch Manager 功能，並在建立此類角色時使用此政策來定義其許可界限。

AWSQuickSetupPatchPolicyPermissionsBoundary 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupPatchPolicyPermissionsBoundary 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：46 UTC
- 編輯時間：2026 年 3 月 5 日 16：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PatchingAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ]
    },
    {
      "Sid" : "PatchingAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "PoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManagedInstanceRoleUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "InstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "InstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "InstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "BaselineS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:Put*",
```

```
        "s3:Get*",
        "s3:List*",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteBucket"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*"
    },
    {
      "Sid" : "PatchingFunctionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "LoggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
```

```
      ]
    },
    {
      "Sid" : "SSMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "EC2TaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "RoleTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
```

```
    {
      "Sid" : "PatchingReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetPatchBaseline",
        "ssm:GetInventory",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAssociation",
        "ssm:GetAutomationExecution",
        "ssm:ListTagsForResource",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PatchingAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/QuickSetup-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:document/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupSchedulerPermissionsBoundary

描述：AWSQuickSetupSchedulerPermissionsBoundary 政策會定義 Quick Setup 所建立的 IAM 角色中允許的許可清單。快速設定使用此政策建立的角色來啟用和設定 Amazon EC2 執行個體和其他資源的排程操作。

AWSQuickSetupSchedulerPermissionsBoundary 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupSchedulerPermissionsBoundary 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：53 UTC
- 編輯時間：2024 年 6 月 26 日 09：53 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ]
    },
    {
      "Sid" : "ConfigurationAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SystemsManagerCalendarReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar-*"
      ]
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2StartStopPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AutomationStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
StartStateManagerAssociations-*"
      ]
    },
    {
      "Sid" : "AssociationsStartOncePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
```

```
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSetupSSMDeploymentRolePolicy

描述：此政策會授予管理權限，允許快速設定建立 Systems Manager 加入程序期間使用的資源。

AWSQuickSetupSSMDeploymentRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupSSMDeploymentRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 15 日 22：53 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
```

```
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-SSM-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunction*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/
AWSQuickSetupSSMLifecycleManagementExecutionPolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupSSMManageResourcesExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources-*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
ExecutionRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
OperationalAccountAdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
```

```
            "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
            "arn:aws:ssm:*::document/AWS-EnableExplorer",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        },
        "StringEquals" : {
```

```
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWSQuickSetupType-SSM-ManageResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeAssociationExecutionTargets",
        "ssm:GetAutomationExecution"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSetupSSMDeploymentS3BucketRolePolicy

描述：此政策授予許可，以列出帳戶中所有 S3 儲存貯體；以及管理及擷取透過 AWS CloudFormation 範本管理之主體帳戶中特定儲存貯體的相關資訊。

AWSQuickSetupSSMDeploymentS3BucketRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupSSMDeploymentS3BucketRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 11 月 15 日 22：01 UTC
- 編輯時間：2024 年 11 月 15 日 22：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentS3BucketRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketTagging",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupSSMHostMgmtPermissionsBoundary

描述：Quick Setup 會建立 IAM 角色，使其能夠代表您設定 Host Manager Quick Setup 類型，並在建立這類角色時使用此政策來定義其許可界限。

AWSQuickSetupSSMHostMgmtPermissionsBoundary 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSetupSSMHostMgmtPermissionsBoundary 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：48 UTC
- 編輯時間：2024 年 6 月 26 日 09：48 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HostManagementAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ]
    },
    {
      "Sid" : "HostManagementAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
```

```
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-HostMgmt-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
CreateAndAttachIAMToInstance-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
UpdateExistingInstanceProfile-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
InstallAndManageCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/AWSEC2-UpdateLaunchAgent-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-GatherSoftwareInventory*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaselineAssociation*",
        "arn:aws:ssm:*:*:automation-definition/AWS-UpdateSSMAgent*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupSSMLifecycleManagementExecutionPolicy

描述：政策會授予管理許可，允許 Quick Setup 在 Systems Manager 的 Quick Setup 部署期間對生命週期事件執行 a AWS CloudFormation 自訂資源。

`AWSQuickSetupSSMLifecycleManagementExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 11 月 15 日 21：55 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC

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

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupSSMManageResourcesExecutionPolicy

描述：此政策授予許可，允許 Systems Manager 建立先決條件，例如 Systems Manager 加入所需的 IAM 角色。

`AWSQuickSetupSSMManageResourcesExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSetupSSMManageResourcesExecutionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 15 日 22：49 UTC
- 編輯時間：2024 年 11 月 15 日 22：49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMManageResourcesExecutionPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableDHMCExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableAREXExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:ListBucketVersions",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSetupStartSSMAssociationsExecutionPolicy

描述：此政策授予許可，允許主體執行啟動 State Manager Associations 的 AWSQuickSetupType-StartSSMAssociations Automation Runbook。

`AWSQuickSetupStartSSMAssociationsExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSetupStartSSMAssociationsExecutionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 8 日 12：04 UTC
- 編輯時間：2026 年 3 月 5 日 16：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
            "arn:aws:ssm:*:*:automation-execution/*",
            "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSetupStartStopInstancesExecutionPolicy

描述：受管政策 AWSQuickSetupStartStopInstancesExecutionPolicy 提供快速設定許可，以排程啟動和停止 Amazon EC2 執行個體。此政策與 Quick Setup 排程器組態類型搭配使用。

`AWSQuickSetupStartStopInstancesExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSetupStartStopInstancesExecutionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 8 日 12：04 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ApplyInstanceState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSightAssetBundleExportPolicy

描述：提供執行 QuickSight 資產套件匯出操作所需的一組許可

`AWSQuickSightAssetBundleExportPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSightAssetBundleExportPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2024 年 3 月 27 日 21：31 UTC
- 編輯時間：2024 年 3 月 27 日 21：31 UTC
- ARN: arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
```

```
    },
    {
      "Sid" : "DataSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:ListRefreshSchedules",
        "quicksight:DescribeDataSetPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "VPCConnectionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeVPCConnection",
        "quicksight:ListVPCConnections"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "RefreshScheduleReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeRefreshSchedule"
```

```
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "AssetBundleExportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleExportJob",
        "quicksight:ListAssetBundleExportJobs",
        "quicksight:StartAssetBundleExportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-export-job/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSightAssetBundleImportPolicy

描述：提供執行 QuickSight 資產套件匯入操作所需的一組許可

`AWSQuickSightAssetBundleImportPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSightAssetBundleImportPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 3 月 27 日 21：40 UTC
- 編輯時間：2024 年 3 月 27 日 21：40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource",
        "quicksight:TagResource",
        "quicksight:UntagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDashboard",
        "quicksight:DeleteDashboard",
        "quicksight:DescribeDashboard",
        "quicksight:UpdateDashboard",
        "quicksight:UpdateDashboardPublishedVersion",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:UpdateDashboardPermissions",
        "quicksight:UpdateDashboardLinks"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateAnalysis",
        "quicksight:DeleteAnalysis",
```

```
        "quicksight:DescribeAnalysis",
        "quicksight:UpdateAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:UpdateAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:DeleteDataSet",
        "quicksight:DescribeDataSet",
        "quicksight:PassDataSet",
        "quicksight:UpdateDataSet",
        "quicksight:DeleteDataSetRefreshProperties",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:PutDataSetRefreshProperties",
        "quicksight:UpdateDataSetPermissions",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:ListRefreshSchedules"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:DescribeDataSource",
        "quicksight:DeleteDataSource",
        "quicksight:PassDataSource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateTheme",
```

```
        "quicksight:DeleteTheme",
        "quicksight:DescribeTheme",
        "quicksight:UpdateTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:UpdateThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "RefreshScheduleWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateRefreshSchedule",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DeleteRefreshSchedule",
        "quicksight:UpdateRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "VPCConnectionWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListVPCConnections",
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "AssetBundleImportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleImportJob",
        "quicksight:ListAssetBundleImportJobs",
        "quicksight:StartAssetBundleImportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuicksightAthenaAccess

描述：Quicksight 存取用於 Athena 查詢結果的 Athena API 和 S3 儲存貯體

AWSQuicksightAthenaAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSQuicksightAthenaAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 12 月 9 日 02：31 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:GetCatalog",
        "glue:GetCatalogs",
        "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" : [
        "*"
      ]
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSightDescribeRDS

描述：允許 QuickSight 描述 RDS 資源

AWSQuickSightDescribeRDS 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSightDescribeRDS 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 11 月 10 日 23：24 UTC
- 編輯時間：2015 年 11 月 10 日 23：24 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Action" : [
        "rds:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSightDescribeRedshift

描述：允許 QuickSight 描述 Redshift 資源

`AWSQuickSightDescribeRedshift` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSightDescribeRedshift` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 11 月 10 日 23：25 UTC
- 編輯時間：2015 年 11 月 10 日 23：25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSightElasticsearchPolicy

描述：提供從 Amazon QuickSight 存取 Amazon Elasticsearch 資源的權限

`AWSQuickSightElasticsearchPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSightElasticsearchPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策

- **建立時間**：2020 年 9 月 9 日 17：27 UTC
- **編輯時間**：2021 年 9 月 7 日，UTC 23：25
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSightIoTAnalyticsAccess

描述：授予 QuickSight 對 IoT Analytics 資料集的唯讀存取權

`AWSQuickSightIoTAnalyticsAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSightIoTAnalyticsAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- **建立時間**：2017 年 11 月 29 日 17：00 UTC
- **編輯時間**：2017 年 11 月 29 日 17：00 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSightListIAM

描述：允許 QuickSight 列出 IAM 實體

`AWSQuickSightListIAM` 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSightListIAM 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 11 月 10 日 23：25 UTC
- 編輯時間：2015 年 11 月 10 日 23：25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuicksightOpenSearchPolicy

描述：提供從 Amazon QuickSight 存取 Amazon OpenSearch 資源的權限

AWSQuicksightOpenSearchPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSQuicksightOpenSearchPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2021 年 9 月 7 日 23：26 UTC
- 編輯時間：2021 年 9 月 7 日 23：26 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSQuickSightSageMakerPolicy

描述：提供從 Amazon QuickSight 存取 Amazon SageMaker 資源的權限 Amazon QuickSight

AWSQuickSightSageMakerPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSightSageMakerPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 1 月 17 日 17：18 UTC
- 編輯時間：2023 年 10 月 30 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:ListModels",
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::quicksight-ml.*",
        "arn:aws:s3:::sagemaker*"
      ]
    },
    {
      "Sid" : "S3ObjectUpdateAccess",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::sagemaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3BucketReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::sagemaker*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSightSecretsManagerWriteAccess

描述：QuickSight 用來在 AWS Secrets Manager 中建立秘密並在現有 QuickSight 秘密上連接資源政策的政策。

AWSQuickSightSecretsManagerWriteAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSQuickSightSecretsManagerWriteAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 5 月 22 日 01：22 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSQuickSightSecretsManagerWriteAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
```

```
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSightSecretsManagerWritePolicy

描述：QuickSight 用來在 AWS Secrets Manager 中建立秘密並在現有 QuickSight 秘密上連接資源政策的政策。

`AWSQuickSightSecretsManagerWritePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSightSecretsManagerWritePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 5 月 12 日 19：22 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightSecretsManagerWritePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSQuickSightTimestreamPolicy

Description： AWS QuickSight 存取 AWS Timestream APIs。客戶可以將此政策連接至 AWS QuickSight 角色，以允許擷取資料和中繼資料。

`AWSQuickSightTimestreamPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSQuickSightTimestreamPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 9 月 30 日，UTC 21：47
- 編輯時間：2020 年 9 月 30 日，UTC 21：47
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSReachabilityAnalyzerServiceRolePolicy

描述：允許 VPC Reachability Analyzer 代表您存取 AWS 資源並與 AWS Organizations 整合。

`AWSReachabilityAnalyzerServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 23 日 17：12 UTC
- 編輯時間：2024 年 9 月 10 日 16：04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReachabilityAnalyzerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
```

```
            "ec2:DescribeInternetGateways",
            "ec2:DescribeManagedPrefixLists",
            "ec2:DescribeNatGateways",
            "ec2:DescribeNetworkAcls",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribePrefixLists",
            "ec2:DescribeRegions",
            "ec2:DescribeRouteTables",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeTransitGatewayAttachments",
            "ec2:DescribeTransitGatewayConnects",
            "ec2:DescribeTransitGatewayPeeringAttachments",
            "ec2:DescribeTransitGatewayRouteTables",
            "ec2:DescribeTransitGatewayVpcAttachments",
            "ec2:DescribeTransitGateways",
            "ec2:DescribeVpcEndpointServiceConfigurations",
            "ec2:DescribeVpcEndpoints",
            "ec2:DescribeVpcPeeringConnections",
            "ec2:DescribeVpcs",
            "ec2:DescribeVpnConnections",
            "ec2:DescribeVpnGateways",
            "ec2:GetManagedPrefixListEntries",
            "ec2:GetTransitGatewayRouteTablePropagations",
            "ec2:SearchTransitGatewayRoutes",
            "elasticloadbalancing:DescribeListeners",
            "elasticloadbalancing:DescribeLoadBalancerAttributes",
            "elasticloadbalancing:DescribeLoadBalancers",
            "elasticloadbalancing:DescribeRules",
            "elasticloadbalancing:DescribeTags",
            "elasticloadbalancing:DescribeTargetGroupAttributes",
            "elasticloadbalancing:DescribeTargetGroups",
            "elasticloadbalancing:DescribeTargetHealth",
            "network-firewall:DescribeFirewall",
            "network-firewall:DescribeFirewallPolicy",
            "network-firewall:DescribeResourcePolicy",
            "network-firewall:DescribeRuleGroup",
            "network-firewall:ListFirewallPolicies",
            "network-firewall:ListFirewalls",
            "network-firewall:ListRuleGroups",
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListAWSServiceAccessForOrganization",
            "organizations:ListAccounts",
```

```
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApigatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSRefactoringToolkitFullAccess

描述：此政策授予許可，以搭配 AWS Toolkit for .NET Refactoring Extension for Microsoft Visual Studio 使用 AWS 服務。它旨在連接到本機 AWS 設定檔。此政策允許上傳應用程式成品，並從 Amazon S3 下載產生的成品。它允許使用 AWS CodeBuild 將應用程式建置到容器映像中，並從 Amazon Elastic Container Registry (Amazon ECR) 儲存和擷取映像。它允許將應用程式部署到 上的容

器服務， AWS 例如 Amazon Elastic Container Service (Amazon ECS)、選用的 VPC 資源建立、選用的現有基礎設施連線，例如 AWS Directory Service，以及其他相關服務。

AWSRefactoringToolkitFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSRefactoringToolkitFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 10 月 25 日 16：41 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupIngress",
            "CreateInternetGateway",
            "CreateKeyPair",
            "CreateRoute",
            "CreateRouteTable",
            "CreateSubnet",
            "CreateVpc"
          ]
        },
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "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"
        }
      }
    },
    {
      "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"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "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"
        }
      }
    },
    {
      "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"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "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"
          ]
        }
      }
    },
    {
      "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"
          ]
        }
      }
    },
    {
      "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"
        }
      }
    },
    {
      "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"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
```

```
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
          ]
        }
      }
    },
    {
      "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" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
    {
      "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" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
```

```
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    },
    {
      "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"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSRefactoringToolkitSidecarPolicy

描述：此政策旨在供建立的 Amazon ECS 任務使用 AWS AWS Toolkit for .NET Refactoring extension for Microsoft Visual Studio 在 中測試應用程式。此政策授予從 Amazon S3 下載應用程式成品的存取權、使用 AWS Systems Manager 和其他必要服務來傳達任務的狀態。

`AWSRefactoringToolkitSidecarPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSRefactoringToolkitSidecarPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 10 月 25 日 16：41 UTC
- 編輯時間：2022 年 10 月 29 日，UTC 22：15
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSrePostPrivateCloudWatchAccess

描述：提供 re：Post 私有存取權以發佈 CloudWatch 指標資料

`AWSrePostPrivateCloudWatchAccess` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 15 日 16：37 UTC
- 編輯時間：2023 年 11 月 15 日 16：37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSRepostSpaceSupportOperationsPolicy

描述：此政策允許 re：Post Space 服務建立、管理和解決透過 Space 應用程式建立的支援案例。

AWSRepostSpaceSupportOperationsPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSRepostSpaceSupportOperationsPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 11 月 26 日 21：52 UTC

- **編輯時間**：2023 年 11 月 26 日 21：52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSResilienceHubAsssessmentExecutionPolicy

描述： AWS Resilience Hub 服務角色的政策，允許存取其他 AWS 服務以執行評估。

AWSResilienceHubAsssessmentExecutionPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSResilienceHubAsssessmentExecutionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 6 月 27 日 12：32 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
```

```
            "cloudformation:DescribeStacks",
            "cloudformation:ListStackResources",
            "cloudformation:ValidateTemplate",
            "cloudwatch:DescribeAlarms",
            "cloudwatch:GetMetricData",
            "cloudwatch:GetMetricStatistics",
            "datasync:DescribeTask",
            "datasync:ListLocations",
            "datasync:ListTasks",
            "devops-guru:ListMonitoredResources",
            "dlm:GetLifecyclePolicies",
            "dlm:GetLifecyclePolicy",
            "docdb-elastic:GetCluster",
            "docdb-elastic:GetClusterSnapshot",
            "docdb-elastic:ListClusterSnapshots",
            "docdb-elastic:ListTagsForResource",
            "drs:DescribeJobs",
            "drs:DescribeSourceServers",
            "drs:GetReplicationConfiguration",
            "ds:DescribeDirectories",
            "dynamodb:DescribeContinuousBackups",
            "dynamodb:DescribeGlobalTable",
            "dynamodb:DescribeLimits",
            "dynamodb:DescribeTable",
            "dynamodb:ListGlobalTables",
            "dynamodb:ListTagsOfResource",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeFastSnapshotRestores",
            "ec2:DescribeFleets",
            "ec2:DescribeHosts",
            "ec2:DescribeInstances",
            "ec2:DescribeNatGateways",
            "ec2:DescribePlacementGroups",
            "ec2:DescribeRegions",
            "ec2:DescribeSnapshots",
            "ec2:DescribeSubnets",
            "ec2:DescribeTags",
            "ec2:DescribeVolumes",
            "ec2:DescribeVpcEndpoints",
            "ecr:DescribeRegistry",
            "ecs:DescribeCapacityProviders",
            "ecs:DescribeClusters",
            "ecs:DescribeContainerInstances",
            "ecs:DescribeServices",
```

```
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeServerlessCacheSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperiment",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListExperimentResolvedTargets",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "rds:ListTagsForResource",
        "resource-groups:GetGroup",
```

```
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:ListBucket",
        "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" : "AWSResilienceHubS3ArtifactStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubS3AccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "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/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSResourceAccessManagerFullAccess

描述：提供 AWS Resource Access Manager 的完整存取權

AWSResourceAccessManagerFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSResourceAccessManagerFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 6 月 4 日 17：28 UTC
- 編輯時間：2019 年 6 月 4 日 17：28 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSResourceAccessManagerReadOnlyAccess

描述：提供 AWS 資源存取管理員的唯讀存取權。

AWSResourceAccessManagerReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSResourceAccessManagerReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 9 日，UTC 20：58
- 編輯時間：2019 年 12 月 9 日 20：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSResourceAccessManagerResourceShareParticipantAccess

描述：提供資源共用參與者所需的 AWS Resource Access Manager APIs存取權。

AWSResourceAccessManagerResourceShareParticipantAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSResourceAccessManagerResourceShareParticipantAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 9 日 20：41 UTC
- 編輯時間：2019 年 12 月 9 日 20：41 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSResourceAccessManagerServiceRolePolicy

描述：包含唯讀 AWS 資源存取管理員存取客戶 Organizations 結構的政策。它也包含可以自行刪除角色的 IAM 許可。

`AWSResourceAccessManagerServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 14 日 19：28 UTC
- 編輯時間：2018 年 11 月 14 日 19：28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSResourceExplorerFullAccess

描述：此政策會授予管理許可來存取 Resource Explorer 資源，並將唯讀許可授予其他 AWS 服務以支援此存取。

AWSResourceExplorerFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSResourceExplorerFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 7 日 20：01 UTC
- 編輯時間：2023 年 11 月 14 日 16：53 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSResourceExplorerOrganizationsAccess

描述：此政策會將管理許可授予 Resource Explorer，並將唯讀許可授予其他 AWS 服務以支援此存取。 AWS Organizations 管理員需要這些許可，才能在 主控台中設定和管理多帳戶搜尋。

`AWSResourceExplorerOrganizationsAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSResourceExplorerOrganizationsAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 11 月 14 日 17：01 UTC
- 編輯時間：2023 年 11 月 14 日 17：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSResourceExplorerReadOnlyAccess

描述：此政策授予唯讀許可，以搜尋和檢視 Resource Explorer 資源，並授予唯讀許可給其他 AWS 服務以支援此存取。

`AWSResourceExplorerReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSResourceExplorerReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 7 日 19：56 UTC
- 編輯時間：2023 年 11 月 14 日 16：43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSResourceExplorerServiceRolePolicy

描述：允許 Resource Explorer 代表您檢視資源和 CloudTrail 事件，為您的資源編製索引以進行搜尋。

`AWSResourceExplorerServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 10 月 25 日，UTC 20：35

- **編輯時間**：2026 年 2 月 27 日 12：12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

政策版本

政策版本： v50 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:DeleteIndex"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel"
      ],
      "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/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "acm:ListCertificates",
        "airflow:ListEnvironments",
        "amplify:ListApps",
```

```
            "amplify:ListBranches",
            "amplify:ListDomainAssociations",
            "aoss:ListCollections",
            "app-integrations:ListApplications",
            "app-integrations:ListEventIntegrations",
            "appconfig:ListApplications",
            "appconfig:ListDeploymentStrategies",
            "appconfig:ListEnvironments",
            "appconfig:ListExtensionAssociations",
            "appflow:ListFlows",
            "appmesh:ListGatewayRoutes",
            "appmesh:ListMeshes",
            "appmesh:ListRoutes",
            "appmesh:ListVirtualGateways",
            "appmesh:ListVirtualNodes",
            "appmesh:ListVirtualRouters",
            "appmesh:ListVirtualServices",
            "apprunner:ListAutoScalingConfigurations",
            "apprunner:ListConnections",
            "apprunner:ListServices",
            "apprunner:ListVpcConnectors",
            "appstream:DescribeAppBlocks",
            "appstream:DescribeApplications",
            "appstream:DescribeFleets",
            "appstream:DescribeImageBuilders",
            "appstream:DescribeStacks",
            "appsync:ListGraphqlApis",
            "aps:ListRuleGroupsNamespaces",
            "aps:ListWorkspaces",
            "athena:ListDataCatalogs",
            "athena:ListWorkGroups",
            "auditmanager:GetAccountStatus",
            "auditmanager:ListAssessments",
            "autoscaling:DescribeAutoScalingGroups",
            "backup-gateway:ListHypervisors",
            "backup:ListBackupPlans",
            "backup:ListBackupVaults",
            "backup:ListRecoveryPointsByBackupVault",
            "backup:ListReportPlans",
            "batch:DescribeComputeEnvironments",
            "batch:DescribeJobDefinitions",
            "batch:DescribeJobQueues",
            "batch:ListSchedulingPolicies",
            "bedrock-agentcore:ListAgentRuntimes",
```

```
        "bedrock:ListAgentAliases",
        "bedrock:ListAgents",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:ViewBudget",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstanceUsers",
        "chime:ListAppInstances",
        "chime:ListMediaInsightsPipelineConfigurations",
        "chime:ListMediaPipelineKinesisVideoStreamPools",
        "chime:ListMediaPipelines",
        "chime:ListSipMediaApplications",
        "chime:ListVoiceConnectors",
        "cleanrooms:ListCollaborations",
        "cloud9:ListEnvironments",
        "cloudformation:ListResources",
        "cloudformation:ListStackSets",
        "cloudformation:ListStacks",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "codeartifact:ListDomains",
        "codeartifact:ListRepositories",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeconnections:ListConnections",
        "codeconnections:ListHosts",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:ListPipelines",
        "codepipeline:ListWebhooks",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "comprehend:ListDocumentClassifiers",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListFlywheels",
        "config:DescribeConfigRules",
        "connect:ListEvaluationForms",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileManualAssignmentQueues",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityProfiles",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
```

```
        "databrew:ListSchedules",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "datapipeline:ListPipelines",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "detective:ListGraphs",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTestGridProjects",
        "directconnect:DescribeDirectConnectGateways",
        "dlm:GetLifecyclePolicies",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTasks",
        "ds:DescribeDirectories",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
```

```
        "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:DescribeTags",
        "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:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSubnetCidrReservations",
```

```
        "ecr-public:DescribeRepositories",
        "ecr:DescribeRepositories",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "emr-containers:ListJobTemplates",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListSecurityConfigurations",
        "emr-containers:ListVirtualClusters",
```

```
        "emr-serverless:ListApplications",
        "es:ListDomainNames",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "fsx:DescribeBackups",
        "fsx:DescribeFileSystems",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
```

```
            "geo:ListTrackers",
            "glacier:ListVaults",
            "globalaccelerator:ListAccelerators",
            "globalaccelerator:ListEndpointGroups",
            "globalaccelerator:ListListeners",
            "glue:GetCrawlers",
            "glue:GetDatabases",
            "glue:GetJobs",
            "glue:GetTables",
            "glue:GetTriggers",
            "glue:ListDataQualityRulesets",
            "glue:ListMLTransforms",
            "glue:ListRegistries",
            "grafana:ListWorkspaces",
            "greengrass:ListComponentVersions",
            "greengrass:ListComponents",
            "greengrass:ListConnectorDefinitions",
            "greengrass:ListCoreDefinitions",
            "greengrass:ListDeviceDefinitions",
            "greengrass:ListFunctionDefinitions",
            "greengrass:ListGroups",
            "greengrass:ListLoggerDefinitions",
            "greengrass:ListResourceDefinitions",
            "greengrass:ListSubscriptionDefinitions",
            "groundstation:ListConfigs",
            "groundstation:ListDataflowEndpointGroups",
            "groundstation:ListMissionProfiles",
            "guardduty:ListDetectors",
            "guardduty:ListFilters",
            "guardduty:ListIPSets",
            "guardduty:ListMalwareProtectionPlans",
            "guardduty:ListPublishingDestinations",
            "guardduty:ListThreatIntelSets",
            "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",
            "inspector2:ListFilters",
            "inspector:ListAssessmentTemplates",
            "iot:ListAuthorizers",
            "iot:ListBillingGroups",
            "iot:ListCACertificates",
            "iot:ListCertificates",
            "iot:ListFleetMetrics",
            "iot:ListJobTemplates",
            "iot:ListJobs",
            "iot:ListMitigationActions",
            "iot:ListPolicies",
            "iot:ListProvisioningTemplates",
            "iot:ListRoleAliases",
            "iot:ListScheduledAudits",
            "iot:ListSecurityProfiles",
            "iot:ListThingGroups",
            "iot:ListThingTypes",
            "iot:ListThings",
            "iot:ListTopicRuleDestinations",
            "iot:ListTopicRules",
            "iotanalytics:ListChannels",
            "iotanalytics:ListDatasets",
            "iotanalytics:ListDatastores",
            "iotanalytics:ListPipelines",
            "iotdeviceadvisor:ListSuiteDefinitions",
            "iotevents:ListAlarmModels",
            "iotevents:ListDetectorModels",
            "iotevents:ListInputs",
            "iotfleethub:ListApplications",
            "iotfleetwise:ListDecoderManifests",
            "iotfleetwise:ListModelManifests",
            "iotfleetwise:ListSignalCatalogs",
            "iotfleetwise:ListVehicles",
            "iotsitewise:ListAccessPolicies",
            "iotsitewise:ListAssetModels",
            "iotsitewise:ListAssets",
```

```
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjects",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:ListClusters",
        "kafka:ListConfigurations",
        "kendra-ranking:ListRescoreExecutionPlans",
        "kendra:ListAccessControlConfigurations",
        "kendra:ListDataSources",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListFeaturedResultsSets",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListThesauri",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kms:ListKeys",
```

```
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayerVersions",
        "lambda:ListLayers",
        "lambda:ListVersionsByFunction",
        "lex:ListBotAliases",
        "lex:ListBots",
        "license-manager:ListDistributedGrants",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:ListTagsForResource",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:ListEnvironments",
        "macie2:ListAllowLists",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "macie2:ListMembers",
        "managedblockchain:ListAccessors",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediastore:ListContainers",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
```

```
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "oam:ListSinks",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListWorkflows",
        "outposts:ListSites",
        "organizations:DescribeResourcePolicy",
        "organizations:ListPolicies",
        "panorama:ListDevices",
        "panorama:ListPackages",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:ListPipes",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceTemplates",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "quicksight:DescribeAccountSubscription",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
```

```
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetResourceShares",
        "ram:ListPermissions",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "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:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeHsmClientCertificates",
        "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-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
```

```
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53domains:ListDomains",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRules",
        "rum:ListAppMonitors",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListImageVersions",
```

```
            "sagemaker:ListImages",
            "sagemaker:ListInferenceComponents",
            "sagemaker:ListInferenceExperiments",
            "sagemaker:ListMlflowTrackingServers",
            "sagemaker:ListModelCardVersions",
            "sagemaker:ListModelCards",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelPackages",
            "sagemaker:ListModels",
            "sagemaker:ListMonitoringSchedules",
            "sagemaker:ListNotebookInstanceLifecycleConfigs",
            "sagemaker:ListNotebookInstances",
            "sagemaker:ListPartnerApps",
            "sagemaker:ListPipelines",
            "sagemaker:ListProjects",
            "sagemaker:ListSpaces",
            "sagemaker:ListStudioLifecycleConfigs",
            "sagemaker:ListTrialComponents",
            "sagemaker:ListTrials",
            "sagemaker:ListUserProfiles",
            "sagemaker:ListWorkforces",
            "sagemaker:ListWorkteams",
            "scheduler:ListScheduleGroups",
            "schemas:ListDiscoverers",
            "secretsmanager:ListSecrets",
            "servicecatalog:ListApplications",
            "servicecatalog:ListAttributeGroups",
            "servicediscovery:ListServices",
            "ses:ListConfigurationSets",
            "ses:ListContactLists",
            "ses:ListDedicatedIpPools",
            "ses:ListEmailIdentities",
            "shield:ListProtectionGroups",
            "shield:ListProtections",
            "signer:ListSigningProfiles",
            "sns:ListTopics",
            "sqs:ListQueues",
            "ssm-incidents:ListResponsePlans",
            "ssm:DescribeInstanceInformation",
            "ssm:DescribeMaintenanceWindowTargets",
            "ssm:DescribeMaintenanceWindowTasks",
            "ssm:DescribeMaintenanceWindows",
            "ssm:DescribeParameters",
            "ssm:DescribeSessions",
```

```
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListFileShares",
        "storagegateway:ListGateways",
        "synthetics:DescribeCanaries",
        "synthetics:ListGroups",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:ListPolicyStores",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTargetGroups",
        "wafv2:ListIPSets",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListRuleGroups",
        "wafv2:ListWebACLs",
        "wellarchitected:ListWorkloads",
        "wisdom:ListAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:ListContents",
        "wisdom:ListKnowledgeBases",
        "workspaces-web:ListPortals",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaces",
        "xray:GetSamplingRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsForReadGetResources",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
```

```
            "backup:ListTags",
            "bedrock-agentcore:GetAgentRuntime",
            "bedrock-agentcore:ListTagsForResource",
            "bedrock:GetAgent",
            "bedrock:GetAgentActionGroup",
            "bedrock:GetAgentCollaborator",
            "bedrock:GetAgentKnowledgeBase",
            "bedrock:GetFlowAlias",
            "bedrock:GetGuardrail",
            "bedrock:GetKnowledgeBase",
            "bedrock:ListAgentActionGroups",
            "bedrock:ListAgentCollaborators",
            "bedrock:ListAgentKnowledgeBases",
            "bedrock:ListTagsForResource",
            "budgets:DescribeBudgetAction",
            "budgets:DescribeBudgetActionsForBudget",
            "cleanrooms:GetCollaboration",
            "cleanrooms:ListMembers",
            "cleanrooms:ListTagsForResource",
            "cloudformation:GetResource",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudtrail:DescribeTrails",
            "cloudtrail:GetEventConfiguration",
            "cloudtrail:GetEventSelectors",
            "cloudtrail:GetInsightSelectors",
            "cloudtrail:GetTrail",
            "cloudtrail:GetTrailStatus",
            "connect:DescribeQueue",
            "dataexchange:GetRevision",
            "dataexchange:ListTagsForResource",
            "dlm:GetLifecyclePolicy",
            "dlm:ListTagsForResource",
            "dynamodb:DescribeContinuousBackups",
            "dynamodb:DescribeContributorInsights",
            "dynamodb:DescribeKinesisStreamingDestination",
            "dynamodb:DescribeTable",
            "dynamodb:DescribeTimeToLive",
            "dynamodb:GetResourcePolicy",
            "dynamodb:ListTagsOfResource",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeVolumeAttribute",
            "ecs:DescribeClusters",
            "ecs:DescribeTaskDefinition",
```

```
        "ecs:ListTagsForResource",
        "eks:DescribeCluster",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:ListDomainsForPackage",
        "es:ListTags",
        "es:ListVpcEndpointsForDomain",
        "events:DescribeRule",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "fis:GetExperiment",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "kendra-ranking:DescribeRescoreExecutionPlan",
        "kendra-ranking:ListTagsForResource",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListTagsForResource",
        "kinesis:ListTagsForStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionScalingConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListTags",
        "logs:DescribeIndexPolicies",
```

```
            "logs:DescribeResourcePolicies",
            "logs:GetDataProtectionPolicy",
            "mediaconnect:DescribeFlow",
            "panorama:DescribeDevice",
            "panorama:ListTagsForResource",
            "ram:GetPermission",
            "rds:ListTagsForResource",
            "redshift:DescribeTags",
            "resource-explorer-2:GetView",
            "route53:GetHostedZone",
            "route53:ListQueryLoggingConfigs",
            "route53:ListTagsForResource",
            "s3:GetAccelerateConfiguration",
            "s3:GetAnalyticsConfiguration",
            "s3:GetBucketAbac",
            "s3:GetBucketCORS",
            "s3:GetBucketLogging",
            "s3:GetBucketMetadataTableConfiguration",
            "s3:GetBucketNotification",
            "s3:GetBucketObjectLockConfiguration",
            "s3:GetBucketOwnershipControls",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketTagging",
            "s3:GetBucketVersioning",
            "s3:GetBucketWebsite",
            "s3:GetEncryptionConfiguration",
            "s3:GetIntelligentTieringConfiguration",
            "s3:GetInventoryConfiguration",
            "s3:GetLifecycleConfiguration",
            "s3:GetMetricsConfiguration",
            "s3:GetReplicationConfiguration",
            "s3:ListTagsForResource",
            "s3express:GetEncryptionConfiguration",
            "s3express:GetLifecycleConfiguration",
            "s3express:ListTagsForResource",
            "sagemaker:DescribeEndpoint",
            "sagemaker:ListTags",
            "secretsmanager:DescribeSecret",
            "sns:GetDataProtectionPolicy",
            "sns:GetTopicAttributes",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTagsForResource",
            "sqs:GetQueueAttributes",
            "sqs:ListQueueTags",
```

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSResourceGroupsReadOnlyAccess

描述：這是 AWS 資源群組的唯讀政策

AWSResourceGroupsReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSResourceGroupsReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 3 月 7 日 10：27 UTC
- 編輯時間：2019 年 2 月 5 日 17：56 UTC
- ARN: arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSRoboMaker_FullAccess

描述：透過 AWS 管理主控台 和 SDK 提供 AWS RoboMaker 的完整存取權。也提供相關服務的選取存取權 （ 例如 S3、IAM)。

AWSRoboMaker_FullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSRoboMaker_FullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 9 月 10 日 18：34 UTC
- 編輯時間：2021 年 9 月 16 日，UTC 21：06
- ARN: arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSRoboMakerReadOnlyAccess

描述：透過 AWS 管理主控台 和 SDK 提供對 AWS RoboMaker 的唯讀存取權

AWSRoboMakerReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSRoboMakerReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 26 日 05：30 UTC
- 編輯時間：2020 年 8 月 28 日，UTC 23：10

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

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSRoboMakerServicePolicy

描述：RoboMaker 服務政策

AWSRoboMakerServicePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 26 日 06：30 UTC
- 編輯時間：2021 年 11 月 11 日 22：23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
```

```
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction",
        "robomaker:CreateSimulationJob",
        "robomaker:CancelSimulationJob"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "robomaker:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration",
        "lambda:DeleteFunction",
        "lambda:ListVersionsByFunction",
        "lambda:GetAlias",
        "lambda:UpdateAlias",
        "lambda:CreateAlias",
        "lambda:DeleteAlias"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "robomaker.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSRoboMakerServiceRolePolicy

描述：RoboMaker 服務政策

AWSRoboMakerServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSRoboMakerServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 26 日 05：33 UTC
- 編輯時間：2018 年 11 月 26 日 05：33 UTC
- ARN: arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSRolesAnywhereFullAccess

描述：提供 IAM Roles Anywhere 資源的所有許可，包括但不限於：CreateProfile、DeleteTrustAnchor、DisableCRL、ResetNotificationSettings。

`AWSRolesAnywhereFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSRolesAnywhereFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 7 月 16 日 14：52 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:CreateTrustAnchor",
        "rolesanywhere:DeleteTrustAnchor",
        "rolesanywhere:DisableTrustAnchor",
        "rolesanywhere:EnableTrustAnchor",
        "rolesanywhere:UpdateTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile",
        "rolesanywhere:CreateProfile",
        "rolesanywhere:DeleteProfile",
        "rolesanywhere:DisableProfile",
        "rolesanywhere:EnableProfile",
        "rolesanywhere:UpdateProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl",
        "rolesanywhere:DeleteCrl",
        "rolesanywhere:DisableCrl",
        "rolesanywhere:EnableCrl",
        "rolesanywhere:ImportCrl",
```

```
        "rolesanywhere:UpdateCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "OtherRolesAnywherePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:PutAttributeMapping",
        "rolesanywhere:DeleteAttributeMapping",
        "rolesanywhere:ResetNotificationSettings",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:TagResource",
        "rolesanywhere:UntagResource",
        "rolesanywhere:PutNotificationSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToRolesAnywhere",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "rolesanywhere.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateRolesAnywhereServiceLinkedRole",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "rolesanywhere.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSRolesAnywhereReadOnly

描述：提供 IAM Roles Anywhere 資源的唯讀許可，包括但不限於：GetTrustAnchor、ListProfiles、GetCRL。此政策中包含的其他服務不會有其他許可。

`AWSRolesAnywhereReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AWSRolesAnywhereReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 7 月 16 日 15：07 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereReadOnly`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
```

```
      ]
    },
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
      "Sid" : "Tags",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSRolesAnywhereServicePolicy

描述：允許 IAM Roles Anywhere 將服務/用量指標發佈至 CloudWatch，並代表您檢查私有憑證授權機構的狀態。

`AWSRolesAnywhereServicePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 7 月 5 日 15：26 UTC
- 編輯時間：2022 年 7 月 5 日 15：26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSS3OnOutpostsServiceRolePolicy

描述：允許 Amazon S3 on Outposts 服務代表您管理 EC2 網路資源。

`AWSS3OnOutpostsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 10 月 3 日 20：32 UTC
- 編輯時間：2023 年 10 月 3 日 20：32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSavingsPlansFullAccess

描述：提供 Savings Plans 服務的完整存取權

AWSSavingsPlansFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSavingsPlansFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 11 月 6 日 22：45 UTC
- 編輯時間：2019 年 11 月 6 日 22：45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSavingsPlansReadOnlyAccess

描述：提供 Savings Plans 服務的唯讀存取權

AWSSavingsPlansReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSavingsPlansReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 11 月 6 日 22：45 UTC
- 編輯時間：2019 年 11 月 6 日 22：45 UTC
- ARN: arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSecretsManagerClientReadOnlyAccess

描述：提供從 Secrets Manager 擷取和描述秘密的存取權。此政策也允許解密 Secrets Manager 秘密的 KMS 金鑰。

`AWSSecretsManagerClientReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSecretsManagerClientReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 11 月 5 日，UTC 20：04
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecretsManagerClientReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Sid" : "SecretsManagerGetAndDescribeSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*"
    },
    {
      "Sid" : "KMSDecryptKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSecurityAgentWebAppPolicy

描述：提供已驗證使用者存取 Security Agent Web Application 的許可，以設定和執行自動化安全滲透測試。此政策可讓使用者管理 pentest、檢視問題清單、監控測試執行，以及與安全測試操作所需的 AWS 資源互動。

`AWSSecurityAgentWebAppPolicy` 是 AWS 受管政策。

使用此政策

您可以將 AWSSecurityAgentWebAppPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2026 年 2 月 5 日 23：19 UTC
- 編輯時間：2026 年 3 月 20 日 17：27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSSecurityAgentWebAppPolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListTargetDomains",
        "securityagent:BatchGetTargetDomains"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "AgentSpaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobTasks",
        "securityagent:CreateDesignReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:GetArtifact",
        "securityagent:DeleteDesignReview",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListPentestJobTasks",
        "securityagent:StartCodeRemediation",
        "securityagent:StartPentestJob",
        "securityagent:StopPentestJob",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest",
        "securityagent:GetDesignReviewFeedback",
        "securityagent:PutDesignReviewFeedback"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSecurityHubFullAccess

描述：提供使用 AWS Security Hub 的完整存取權。

`AWSSecurityHubFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSecurityHubFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 27 日，UTC 23：54
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "securityhub.amazonaws.com",
            "securityhubv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:UpdateDetector",
        "guardduty:EnableOrganizationAdminAccount",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:DeleteDetector",
        "guardduty:CreateDetector",
        "guardduty:CreateMembers",
        "guardduty:UpdateOrganizationConfiguration",
        "guardduty:DescribeOrganizationConfiguration",
        "inspector2:BatchGetAccountStatus",
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:DisableDelegatedAdminAccount",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:UpdateOrganizationConfiguration",
        "inspector2:DescribeOrganizationConfiguration",
        "pricing:GetProducts",
        "account:ListRegions",
```

```
        "account:GetRegionOptStatus",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSecurityHubOrganizationsAccess

描述：授予在組織內啟用和管理 AWS Security Hub 的許可。包括在整個組織中啟用服務，以及判斷服務的委派管理員帳戶。

`AWSSecurityHubOrganizationsAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSecurityHubOrganizationsAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2021 年 3 月 15 日 20：53 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:ListParents",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource" : [
        "arn:aws:organizations::*:root/o-*/*",
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
```

```
          "organizations:PolicyType" : [
            "SECURITYHUB_POLICY",
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSecurityHubReadOnlyAccess

描述：提供 AWS Security Hub 資源的唯讀存取權

`AWSSecurityHubReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSecurityHubReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 11 月 28 日 01：34 UTC
- 編輯時間：2024 年 2 月 22 日 23：45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSecurityHubServiceRolePolicy

描述： AWS Security Hub 存取 資源所需的服務連結角色。

AWSSecurityHubServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 27 日，UTC 23：47
- 編輯時間：2023 年 11 月 27 日 03：46 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSSecurityHubV2ServiceRolePolicy

描述：此政策允許 Security Hub 代表您管理組織中的 AWS Config 規則和 Security Hub 資源。

AWSSecurityHubV2ServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 6 月 10 日 17：37 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubV2ServiceRolePolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssets/*",
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssetsGlobal/*"
      ]
    },
```

```
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleSecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DisableSecurityHubV2",
        "securityhub:EnableSecurityHubV2",
        "securityhub:DescribeSecurityHubV2"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hubv2/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsOnResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
```

```
      "Resource" : "arn:aws:organizations::*:*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsWithoutResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleDelegatedAdminPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleEcrListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeImages",
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaMetricPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIamListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetAccountSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSecurityIncidentResponseCaseFullAccess

描述：政策提供客戶透過安全事件回應服務建立的案例資源的讀取和寫入許可。

AWSSecurityIncidentResponseCaseFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSecurityIncidentResponseCaseFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 1 日 23：21 UTC

- **編輯時間**：2026 年 2 月 12 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseCaseFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRCaseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRCaseTagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIRCaseWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
```

```
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityIRCaseTagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSecurityIncidentResponseFullAccess

描述：政策可為客戶提供與安全事件回應服務相關聯的所有資源的讀取和寫入許可。

AWSSecurityIncidentResponseFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSecurityIncidentResponseFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 1 日 23：21 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSSecurityIncidentResponseFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetMembership",
        "security-ir:ListMemberships",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SecurityIRWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "security-ir:CancelMembership",
        "security-ir:CreateCase",
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment",
        "security-ir:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponse",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponseTriage",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/triage.security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse_Triage"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSecurityIncidentResponseReadOnlyAccess

描述：政策可為客戶提供與安全事件回應服務相關聯的所有資源的唯讀許可。許可包括存取 GetCaseAttachmentDownloadUrl，以及取得案例連接下載 URLs的功能。

AWSSecurityIncidentResponseReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSecurityIncidentResponseReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 1 日 23：06 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AWSSecurityIncidentResponseReadOnlyAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetMembership",
        "security-ir:ListMemberships",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSecurityIncidentResponseServiceRolePolicy

描述：提供存取由安全事件回應管理或使用 AWS 的資源

AWSSecurityIncidentResponseServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 12 月 1 日 16：36 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseServiceRolePolicy

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIncidentResponseOrganizationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIncidentResponseCreateCasePolicyTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:CreateCase"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      },
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIncidentResponseOperationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:UpdateCase",
        "security-ir:ListCases",
```

```
        "security-ir:CreateCaseComment",
        "security-ir:ListComments"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSecurityIncidentResponseTriageServiceRolePolicy

描述：提供 AWS 安全事件回應的存取權，以持續監控您的環境是否有安全威脅、調校安全服務以減少警示雜訊，以及收集資訊以調查潛在事件。

AWSSecurityIncidentResponseTriageServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 12 月 1 日 16：36 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseTriageServiceRolePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:CreateFilter",
        "guardduty:DescribeMalwareScans",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
```

```
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:StartMalwareScan",
        "guardduty:UpdateFindingsFeedback"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:BatchUpdateFindings",
        "securityhub:DescribeHub",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindings",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:UpdateFindings"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
        "security-ir:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:UpdateCase"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetMembership",
        "security-ir:ListMemberships"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceCatalogAdminFullAccess

描述：提供服務目錄管理功能的完整存取權

AWSServiceCatalogAdminFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSServiceCatalogAdminFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 2 月 15 日 17：19 UTC
- 編輯時間：2023 年 4 月 13 日 18：43 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceCatalogAdminReadOnlyAccess

描述：提供 Service Catalog 管理功能的唯讀存取權

AWSServiceCatalogAdminReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSServiceCatalogAdminReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 10 月 25 日 18：53 UTC
- 編輯時間：2019 年 10 月 25 日 18：53 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceCatalogAppRegistryFullAccess

描述：提供 Service Catalog App Registry 功能的完整存取權

AWSServiceCatalogAppRegistryFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSServiceCatalogAppRegistryFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 11 月 12 日 22：25 UTC
- 編輯時間：2023 年 12 月 7 日 21：50 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceCatalogAppRegistryReadOnlyAccess

描述：提供 Service Catalog 應用程式登錄檔功能的唯讀存取權

AWSServiceCatalogAppRegistryReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSServiceCatalogAppRegistryReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 11 月 12 日 22：34 UTC
- 編輯時間：2022 年 11 月 17 日 18：16 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceCatalogAppRegistryServiceRolePolicy

描述：允許 Service Catalog AppRegistry 代表您管理資源群組

`AWSServiceCatalogAppRegistryServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 5 月 18 日，UTC 22：18
- 編輯時間：2022 年 10 月 26 日 16：05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceCatalogEndUserFullAccess

描述：提供服務目錄最終使用者功能的完整存取權

AWSServiceCatalogEndUserFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSServiceCatalogEndUserFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 2 月 15 日 17：22 UTC
- 編輯時間：2019 年 7 月 10 日 20：30 UTC
- ARN: arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSServiceCatalogEndUserReadOnlyAccess

描述：提供 Service Catalog 最終使用者功能的唯讀存取權

`AWSServiceCatalogEndUserReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSServiceCatalogEndUserReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 10 月 25 日 18：49 UTC
- 編輯時間：2019 年 10 月 25 日 18：49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

描述： AWS ServiceCatalog 的服務連結角色政策，可與 AWS Organizations 組織結構同步

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 4 月 10 日 20：48 UTC
- 編輯時間：2025 年 12 月 8 日 19：04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "OrganizationsDataSyncToServiceCatalogRegions",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSServiceCatalogSyncServiceRolePolicy

描述： AWS ServiceCatalog 的服務連結角色，用於從來源儲存庫同步佈建成品

AWSServiceCatalogSyncServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 15 日 21：20 UTC
- 編輯時間：2024 年 5 月 3 日 17：12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
```

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForAIDevOpsPolicy

描述：此服務連結角色提供 AIDevOps 提供用量資訊的能力。

AWSServiceRoleForAIDevOpsPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2026 年 2 月 16 日 14：27 UTC
- 編輯時間：2026 年 2 月 16 日 14：27 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAIDevOpsPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AIDevOps"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSServiceRoleForAmazonEKSNodegroup

描述：管理客戶帳戶中節點群組所需的許可。這些政策與下列資源的管理相關：AutoscalingGroups、SecurityGroups、 LaunchTemplates 和 InstanceProfiles。

`AWSServiceRoleForAmazonEKSNodegroup` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 7 日 01：34 UTC
- 編輯時間：2026 年 2 月 17 日 18：42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
```

```
        "autoscaling:PutWarmPool",
        "autoscaling:DeleteWarmPool"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
    },
    {
      "Sid" : "AllowAutoscalingToCreateSLR",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      },
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowASGCreationByEKS",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "autoscaling.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToManageResourcesForNodegroups",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "ec2:CreateLaunchTemplate",
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "ec2:DescribeLaunchTemplates",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RunInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:GetConsoleOutput",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeCapacityReservations",
        "autoscaling:DescribeWarmPool"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
```

```
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
    },
    {
      "Sid" : "PermissionsToDeleteEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsForManagedNodegroupsAutoRepair",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreateEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*",
        "arn:*:ec2:*:*:launch-template/*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingEC2ResourcesOnlyDuringInstanceCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:instance/*",
        "arn:*:ec2:*:*:volume/*",
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForAmazonQDeveloper

描述：此服務連結角色可讓 Amazon Q Developer 提供用量資訊。

AWSServiceRoleForAmazonQDeveloper 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 4 月 25 日 07：40 UTC
- 編輯時間：2024 年 4 月 25 日 07：40 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForAWSTransform

描述：此服務連結角色可讓 AWS Transform 提供用量資訊。

AWSServiceRoleForAWSTransform 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 5 月 15 日 13：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransform

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Transform"
          ]
        }
      }
    },
    {
      "Sid" : "UserManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:ListApplicationAssignmentsForPrincipal"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SupportCaseManagement",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:AddCommunicationToCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExternalIdpSecretsAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:transform!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

描述：提供存取 CloudWatch 警示使用的 Systems Manager 資源

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 10 月 1 日 09：49 UTC
- 編輯時間：2020 年 10 月 1 日，UTC 09：49
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

描述：允許 CloudWatch 代表您存取 RDS Performance Insights 指標

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 9 月 7 日 09：32 UTC
- 編輯時間：2023 年 9 月 7 日 09：32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForCodeGuru-Profiler

描述：Amazon CodeGuru Profiler 代表您傳送通知所需的服務連結角色。

`AWSServiceRoleForCodeGuru-Profiler` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 6 月 26 日 22：04 UTC
- 編輯時間：2020 年 6 月 26 日，22：04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForCodeWhispererPolicy

描述：此角色授予 CodeWhisperer 許可，以存取您帳戶中的資料來計算帳單、提供在 Amazon CodeGuru 中建立和存取安全報告的存取權，以及將資料傳送到 CloudWatch。

`AWSServiceRoleForCodeWhispererPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 3 月 24 日 19：39 UTC
- 編輯時間：2024 年 3 月 29 日 22：13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance",
        "sso:DescribeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid3",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateUploadUrl"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid4",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
```

```
        "codeguru-security:GetFindings"
      ],
      "Resource" : [
        "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
      ]
    },
    {
      "Sid" : "sid5",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/CodeWhisperer"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForEC2ScheduledInstances

描述：允許 EC2 排程執行個體啟動和管理 Spot 執行個體。

`AWSServiceRoleForEC2ScheduledInstances` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 10 月 12 日 18：31 UTC
- 編輯時間：2017 年 10 月 12 日 18：31 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Description： AWS GroundStation 使用此服務連結角色來叫用 EC2 以尋找公有 IPv4 地址

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 12 月 13 日，UTC 23：52
- 編輯時間：2022 年 12 月 13 日 23：52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForImageBuilder

描述：允許 EC2ImageBuilder 代表您呼叫 AWS 服務。

`AWSServiceRoleForImageBuilder` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 29 日，UTC 22：02
- 編輯時間：2026 年 3 月 17 日 20：42 UTC

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

政策版本

政策版本： v27 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "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: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-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "imagebuilder:StartImagePipelineExecution",
      "Resource" : "arn:aws:imagebuilder:*:*:image-pipeline/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "imagebuilder:TagResource",
      "Resource" : "arn:aws:imagebuilder:*:*:image-pipeline/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForIoTSiteWise

描述：允許 AWS IoT SiteWise 佈建和管理閘道以及查詢資料。此政策包含部署至 群組所需的 AWS Greengrass 許可、建立和更新服務字首函數的 AWS Lambda 許可，以及從資料存放區查詢資料的 AWS IoT Analytics 許可。

`AWSServiceRoleForIoTSiteWise` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 14 日，UTC 19：19
- 編輯時間：2023 年 11 月 13 日 18：27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSServiceRoleForLogDeliveryPolicy

描述：允許 Log Delivery 服務代表您呼叫日誌目的地來交付日誌。

`AWSServiceRoleForLogDeliveryPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 10 月 4 日 17：31 UTC
- 編輯時間：2025 年 1 月 16 日 21：37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogDeliveryToFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForMonitronPolicy

描述：授予 Amazon Monitron 管理 AWS 資源的許可，包括代表您指派 AWS SSO 使用者。

`AWSServiceRoleForMonitronPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 2 日 19：06 UTC
- 編輯時間：2026 年 1 月 7 日 09：34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "sso:CreateApplicationAssignment",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForNeptuneGraphPolicy

描述：提供 Cloudwatch 存取權，以發佈 Amazon Neptune 的操作和用量指標和日誌

AWSServiceRoleForNeptuneGraphPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 29 日 14：03 UTC
- 編輯時間：2023 年 11 月 29 日 14：03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRoleForPrivateMarketplaceAdminPolicy

描述：提供描述和更新 Private Marketplace 資源以及描述 AWS Organizations 的許可

`AWSServiceRoleForPrivateMarketplaceAdminPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 2 月 14 日 22：28 UTC
- 編輯時間：2024 年 2 月 14 日 22：28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSServiceRoleForProcurementInsightsPolicy

描述：採購詳情取得組織帳戶詳細資訊的政策

AWSServiceRoleForProcurementInsightsPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 10 月 3 日 14：26 UTC
- 編輯時間：2024 年 10 月 3 日 14：26 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForProcurementInsightsPolicy

政策版本

政策版本： v1 （ 預設 ）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSServiceRoleForSMS

描述：提供將 AWS 服務執行個體遷移至 所需的 服務和資源的存取權， AWS 包括 EC2, S3 和 Cloudformation。

AWSServiceRoleForSMS 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 8 月 6 日 18：39 UTC
- 編輯時間：2020 年 10 月 15 日 17：28 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSServiceRoleForUserSubscriptions

描述：提供對 Identity Center 資源的使用者訂閱服務的存取權，以自動更新您的訂閱。

`AWSServiceRoleForUserSubscriptions` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 4 月 25 日 16：14 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SubscriptionManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "organizations:DescribeOrganization",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso-directory:DescribeUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRolePolicyForBackupReports

描述：提供 AWS 備份許可，以代表您建立合規報告

AWSServiceRolePolicyForBackupReports 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 8 月 19 日，UTC 21：16
- 編輯時間：2023 年 3 月 10 日 00：51 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRolePolicyForBackupRestoreTesting

描述：此政策包含測試還原和清除測試期間建立之資源的許可。

AWSServiceRolePolicyForBackupRestoreTesting 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 10 日 23：37 UTC
- 編輯時間：2026 年 3 月 18 日 22：12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "rds:DeleteTenantDatabase",
        "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-*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSServiceRolePolicyForWorkspacesInstances

描述：此受管政策提供 Amazon WorkSpaces 的管理存取權，以管理 中的 EC2 執行個體 AWS 帳戶

AWSServiceRolePolicyForWorkspacesInstances 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 6 月 11 日 20：37 UTC
- 編輯時間：2025 年 6 月 11 日 20：37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForWorkspacesInstances

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ManagedResourceOperator" : "workspaces-instances.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSShieldDRTAccessPolicy

描述：為 AWS DDoS 回應團隊提供對 的有限存取權 AWS 帳戶 ，以協助在高嚴重性事件期間緩解 DDoS 攻擊。

AWSShieldDRTAccessPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSShieldDRTAccessPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 6 月 5 日，UTC 22：29
- 編輯時間：2020 年 12 月 15 日 17：28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSShieldServiceRolePolicy

描述：允許 AWS Shield 代表您存取 AWS 資源，以提供 DDoS 保護。

AWSShieldServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 11 月 17 日 19：17 UTC
- 編輯時間：2021 年 11 月 17 日 19：17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSocialMessagingServiceRolePolicy

描述：提供發佈指標的存取權，並提供社交訊息傳送的洞見。

AWSSocialMessagingServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 10 月 10 日 19：28 UTC
- 編輯時間：2024 年 10 月 10 日 19：28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSocialMessagingServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSSMForSAPServiceLinkedRolePolicy

描述：為 AWS Systems Manager for SAP 提供管理與整合 SAP 軟體所需的許可 AWS。

AWSSSMForSAPServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 16 日 01：18 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy

政策版本

政策版本： v21 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "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:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
```

```
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    },
    {
      "Sid" : "StartStopInstances",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "SsmSapResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag",
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEc2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPManaged" : "True"
        },
        "ForAllValues:StringLike" : {
```

```
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageAppTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/awsApplication" : "arn:aws:resource-groups:*:*:group/*/*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "awsApplication"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCostAllocationTags",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:StartCostAllocationTagBackfill"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSSSMOpsInsightsServiceRolePolicy

描述：服務連結角色 AWSServiceRoleForAmazonSSM_OpsInsights 的政策

`AWSSSMOpsInsightsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 6 月 16 日 20：12 UTC
- 編輯時間：2021 年 6 月 16 日 20：12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSSSODirectoryAdministrator

描述：SSO 目錄的管理員存取權

AWSSSODirectoryAdministrator 是 AWS 受管政策。

使用此政策

您可以將 AWSSSODirectoryAdministrator 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 10 月 31 日，UTC 23：54
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSSODirectoryReadOnly

描述：SSO 目錄的 ReadOnly 存取

`AWSSSODirectoryReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSSODirectoryReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2018 年 10 月 31 日，UTC 23：49
- **編輯時間**：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
```

```
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSSOMasterAccountAdministrator

描述：在 AWS SSO 內提供存取權，以管理 AWS Organizations 主帳戶、成員帳戶和雲端應用程式

`AWSSSOMasterAccountAdministrator` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSSOMasterAccountAdministrator` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 6 月 27 日 20：36 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSSOMemberAccountAdministrator

描述：在 AWS SSO 內提供存取權，以管理 AWS Organizations 成員帳戶和雲端應用程式

AWSSSOMemberAccountAdministrator 是 AWS 受管政策。

使用此政策

您可以將 AWSSSOMemberAccountAdministrator 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 6 月 27 日，UTC 20：45
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
```

```
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
```

```
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSSOReadOnly

描述：提供 AWS SSO 組態的唯讀存取權。

AWSSSOReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSSSOReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 6 月 27 日，UTC 20：24
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AWSSSOReadOnly

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
```

```
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSSOServiceRolePolicy

描述：授予 AWS SSO 許可來代表您管理 AWS 資源，包括 IAM 角色、政策和 SAML IdP。

AWSSSOServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 12 月 5 日 18：36 UTC
- 編輯時間：2025 年 2 月 11 日 18：37 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy

政策版本

政策版本： v18 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSStepFunctionsConsoleFullAccess

描述：為user/role/etc提供 AWS StepFunctions 主控台存取權的存取政策。為了獲得完整的主控台體驗，除了此政策之外，使用者可能需要服務可擔任之其他 IAM 角色的 iam：PassRole 許可。

`AWSStepFunctionsConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSStepFunctionsConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 1 月 11 日 21：54 UTC
- 編輯時間：2017 年 1 月 12 日 00：19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSStepFunctionsFullAccess

描述：提供user/role/etc存取給 AWS StepFunctions API 的存取政策。若要完整存取，除了此政策之外，使用者必須擁有至少一個可由服務擔任之 IAM 角色的 iam：PassRole 許可。

`AWSStepFunctionsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSStepFunctionsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 1 月 11 日 21：51 UTC
- 編輯時間：2017 年 1 月 11 日 21：51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSStepFunctionsReadOnlyAccess

描述：一種存取政策，提供user/role/etc對 AWS StepFunctions 服務的唯讀存取權。

`AWSStepFunctionsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSStepFunctionsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 1 月 11 日 21：46 UTC
- 編輯時間：2024 年 4 月 26 日 18：53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:DescribeActivity",
        "states:ListTagsForResource",
        "states:DescribeMapRun",
        "states:ListMapRuns",
        "states:DescribeStateMachineAlias",
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ValidateStateMachineDefinition"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSStorageGatewayFullAccess

描述：透過 提供 AWS Storage Gateway的完整存取權 AWS 管理主控台。

AWSStorageGatewayFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSStorageGatewayFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2022 年 9 月 6 日 20：26 UTC
- ARN: arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSStorageGatewayReadOnlyAccess

描述：透過 提供對 AWS Storage Gateway的存取 AWS 管理主控台。

`AWSStorageGatewayReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSStorageGatewayReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2022 年 9 月 6 日 20：24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSStorageGatewayServiceRolePolicy

描述： AWS Storage Gateway 用來啟用其他 AWS 服務與 Storage Gateway 整合的服務連結角色。

AWSStorageGatewayServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 2 月 17 日 19：03 UTC
- 編輯時間：2021 年 2 月 17 日 19：03 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSupplyChainFederationAdminAccess

描述：AWSSupplyChainFederationAdminAccess 提供 AWS Supply Chain 聯合身分使用者存取 AWS Supply Chain 應用程式的權限，包括在 AWS Supply Chain 應用程式中執行動作所需的許可。此政策透過 IAM Identity Center 使用者和群組提供管理許可，並連接至 AWS 由 Supply Chain 代表您建立的角色。您不應將 AWSSupplyChainFederationAdminAccess 政策連接至任何其他 IAM 實體。

`AWSSupplyChainFederationAdminAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSupplyChainFederationAdminAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 3 月 1 日 18：54 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "sso:ListApplicationAssignments",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationAssignmentConfiguration"
      ],
      "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"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSupportAccess

描述：允許使用者存取 AWS 支援 中心。

AWSSupportAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSupportAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AWSSupportAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSupportAppFullAccess

描述：提供 AWS 支援 應用程式和其他必要服務的完整存取權，例如 AWS 支援 和 Service Quotas。此政策包含使用支援服務的許可，讓使用者可以聯絡 AWS 支援 以取得支援案例、變更服務配額，以及建立相關的服務連結角色。

AWSSupportAppFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSupportAppFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 8 月 22 日 16：53 UTC
- 編輯時間：2022 年 8 月 22 日 16：53 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSupportAppReadOnlyAccess

描述：提供 AWS 支援 應用程式的唯讀存取權。

`AWSSupportAppReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSupportAppReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 8 月 22 日 17：01 UTC
- 編輯時間：2022 年 8 月 22 日 17：01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSupportPlansFullAccess

描述：提供 Supportplans 的完整存取權。

AWSSupportPlansFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSupportPlansFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 9 月 27 日 18：19 UTC
- 編輯時間：2024 年 9 月 9 日，UTC 21：15
- ARN: arn:aws:iam::aws:policy/AWSSupportPlansFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSupportPlansReadOnlyAccess

描述：提供 Supportplans 的唯讀存取權。

`AWSSupportPlansReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSupportPlansReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 9 月 27 日 18：08 UTC
- 編輯時間：2024 年 9 月 9 日 21：21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSupportServiceRolePolicy

描述：允許 AWS 支援 存取 AWS 資源以提供帳單、管理和支援服務。

AWSSupportServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 4 月 19 日，UTC 18：04
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy

政策版本

政策版本： v56 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "AWSSupportActionsGroup1",
      "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",
        "account:getRegionOptStatus",
        "account:listRegions",
        "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",
            "aiops:getInvestigationGroup",
            "aiops:getInvestigationGroupPolicy",
            "aiops:listInvestigationGroups",
            "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:listJobs",
            "amplify:listWebhooks",
            "amplifyuibuilder:exportComponents",
            "amplifyuibuilder:exportThemes",
            "aoss:batchGetCollection",
            "aoss:batchGetEffectiveLifecyclePolicy",
            "aoss:batchGetLifecyclePolicy",
            "aoss:batchGetVpcEndpoint",
            "aoss:getAccessPolicy",
            "aoss:getAccountSettings",
            "aoss:getPoliciesStats",
            "aoss:getSecurityConfig",
            "aoss:getSecurityPolicy",
            "aoss:listAccessPolicies",
            "aoss:listCollections",
            "aoss:listLifecyclePolicies",
            "aoss:listSecurityConfigs",
            "aoss:listSecurityPolicies",
            "aoss:listTagsForResource",
            "aoss:listVpcEndpoints",
            "appconfig:getApplication",
            "appconfig:getConfigurationProfile",
            "appconfig:getDeployment",
            "appconfig:getDeploymentStrategy",
            "appconfig:getEnvironment",
            "appconfig:getExtension",
            "appconfig:getExtensionAssociation",
```

```
            "appconfig:listApplications",
            "appconfig:listConfigurationProfiles",
            "appconfig:listDeployments",
            "appconfig:listDeploymentStrategies",
            "appconfig:listEnvironments",
            "appconfig:listExtensionAssociations",
            "appconfig:listExtensions",
            "appconfig:listHostedConfigurationVersions",
            "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",
            "application-signals:getService",
            "application-signals:getServiceLevelObjective",
            "application-signals:listServiceDependencies",
            "application-signals:listServiceDependents",
            "application-signals:listServiceLevelObjectives",
            "application-signals:listServiceOperations",
            "application-signals:listServices",
            "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:describeObservabilityConfiguration",
            "apprunner:describeOperation",
            "apprunner:describeService",
            "apprunner:describeVpcConnector",
            "apprunner:describeVpcIngressConnection",
            "apprunner:listAutoScalingConfigurations",
            "apprunner:listConnections",
            "apprunner:listObservabilityConfigurations",
            "apprunner:listOperations",
            "apprunner:listServices",
            "apprunner:listTagsForResource",
            "apprunner:listVpcConnectors",
            "apprunner:listVpcIngressConnections",
            "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:evaluateCode",
        "appsync:evaluateMappingTemplate",
        "appsync:getApi",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getChannelNamespace",
        "appsync:getDataSource",
        "appsync:getDataSourceIntrospection",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getGraphqlApiEnvironmentVariables",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listApis",
        "appsync:listChannelNamespaces",
        "appsync:listDataSources",
        "appsync:listDomainNames",
        "appsync:listFunctions",
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
        "aps:describeRuleGroupsNamespace",
        "aps:describeScraper",
        "aps:describeWorkspace",
        "aps:listRuleGroupsNamespaces",
        "aps:listScrapers",
        "aps:listWorkspaces",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getCapacityAssignmentConfiguration",
        "athena:getCapacityReservation",
        "athena:getDataCatalog",
```

```
            "athena:getNamedQuery",
            "athena:getNotebookMetadata",
            "athena:getQueryExecution",
            "athena:getQueryRuntimeStatistics",
            "athena:getSession",
            "athena:getSessionStatus",
            "athena:getWorkGroup",
            "athena:listApplicationDPUSizes",
            "athena:listCalculationExecutions",
            "athena:listCapacityReservations",
            "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:describeTrafficSources",
        "autoscaling:describeWarmPool",
        "backup-gateway:getBandwidthRateLimitSchedule",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup-search:listSearchJobBackups",
        "backup-search:listSearchJobs",
        "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:getRecoveryPointIndexDetails",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
```

```
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listIndexedRecoveryPoints",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "batch:describeComputeEnvironments",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:describeSchedulingPolicies",
        "batch:listJobs",
        "bedrock:getAgent",
        "bedrock:getAgentActionGroup",
        "bedrock:getAgentAlias",
        "bedrock:getAgentKnowledgeBase",
        "bedrock:getAgentVersion",
        "bedrock:getAutomatedReasoningPolicy",
        "bedrock:getAutomatedReasoningPolicyAnnotations",
        "bedrock:getAutomatedReasoningPolicyBuildWorkflow",
        "bedrock:getAutomatedReasoningPolicyBuildWorkflowResultAssets",
        "bedrock:getAutomatedReasoningPolicyNextScenario",
        "bedrock:getAutomatedReasoningPolicyTestCase",
        "bedrock:getAutomatedReasoningPolicyTestResult",
        "bedrock:getCustomModel",
        "bedrock:getDataSource",
        "bedrock:getEvaluationJob",
        "bedrock:getFlow",
        "bedrock:getFlowAlias",
        "bedrock:getFlowVersion",
```

```
            "bedrock:getFoundationModel",
            "bedrock:getGuardrail",
            "bedrock:getImportedModel",
            "bedrock:getInferenceProfile",
            "bedrock:getIngestionJob",
            "bedrock:getKnowledgeBase",
            "bedrock:getMarketplaceModelEndpoint",
            "bedrock:getModelCopyJob",
            "bedrock:getModelCustomizationJob",
            "bedrock:getModelImportJob",
            "bedrock:getModelInvocationJob",
            "bedrock:getModelInvocationLoggingConfiguration",
            "bedrock:getPrompt",
            "bedrock:getPromptRouter",
            "bedrock:getProvisionedModelThroughput",
            "bedrock:listAgentActionGroups",
            "bedrock:listAgentAliases",
            "bedrock:listAgentKnowledgeBases",
            "bedrock:listAgents",
            "bedrock:listAgentVersions",
            "bedrock:listAutomatedReasoningPolicies",
            "bedrock:listAutomatedReasoningPolicyBuildWorkflows",
            "bedrock:listAutomatedReasoningPolicyTestCases",
            "bedrock:listAutomatedReasoningPolicyTestResults",
            "bedrock:listCustomModels",
            "bedrock:listDataSources",
            "bedrock:listEvaluationJobs",
            "bedrock:exportAutomatedReasoningPolicyVersion",
            "bedrock:listFlowAliases",
            "bedrock:listFlows",
            "bedrock:listFlowVersions",
            "bedrock:listFoundationModels",
            "bedrock:listGuardrails",
            "bedrock:listImportedModels",
            "bedrock:listInferenceProfiles",
            "bedrock:listIngestionJobs",
            "bedrock:listKnowledgeBases",
            "bedrock:listMarketplaceModelEndpoints",
            "bedrock:listModelCopyJobs",
            "bedrock:listModelCustomizationJobs",
            "bedrock:listModelImportJobs",
            "bedrock:listModelInvocationJobs",
            "bedrock:listPromptRouters",
            "bedrock:listPrompts",
```

```
        "bedrock:listProvisionedModelThroughputs",
        "braket:getDevice",
        "braket:getJob",
        "braket:getQuantumTask",
        "braket:getServiceLinkedRoleStatus",
        "braket:getUserAgreementStatus",
        "braket:searchDevices",
        "braket:searchJobs",
        "braket:searchQuantumTasks",
        "braket:searchSpendingLimits",
        "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:getCollaborationConfiguredAudienceModelAssociation",
            "cleanrooms:getCollaborationPrivacyBudgetTemplate",
            "cleanrooms:getConfiguredTable",
            "cleanrooms:getConfiguredTableAnalysisRule",
            "cleanrooms:getConfiguredTableAssociation",
            "cleanrooms:getConfiguredAudienceModelAssociation",
            "cleanrooms:getMembership",
            "cleanrooms:getPrivacyBudgetTemplate",
            "cleanrooms:getSchema",
            "cleanrooms:getSchemaAnalysisRule",
            "cleanrooms:listAnalysisTemplates",
            "cleanrooms:listCollaborationAnalysisTemplates",
            "cleanrooms:listCollaborationConfiguredAudienceModelAssociations",
            "cleanrooms:listCollaborationPrivacyBudgetTemplates",
            "cleanrooms:listCollaborationPrivacyBudgets",
            "cleanrooms:listCollaborations",
            "cleanrooms:listConfiguredAudienceModelAssociations",
            "cleanrooms:listConfiguredTableAssociations",
            "cleanrooms:listConfiguredTables",
            "cleanrooms:listMembers",
            "cleanrooms:listMemberships",
            "cleanrooms:listPrivacyBudgetTemplates",
            "cleanrooms:listPrivacyBudgets",
            "cleanrooms:listProtectedQueries",
            "cleanrooms:listSchemas",
            "cleanrooms:previewPrivacyImpact",
            "cloud9:describeEnvironmentMemberships",
            "cloud9:describeEnvironments",
            "cloud9:listEnvironments",
            "clouddirectory:getDirectory",
            "clouddirectory:listDirectories",
            "cloudformation:batchDescribeTypeConfigurations",
            "cloudformation:describeAccountLimits",
            "cloudformation:describeChangeSet",
            "cloudformation:describeChangeSetHooks",
```

```
        "cloudformation:describePublisher",
        "cloudformation:describeStackDriftDetectionStatus",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResourceDrifts",
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getResource",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listResources",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeFunction",
        "cloudfront:describeKeyValueStore",
        "cloudfront:getAnycastIpList",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
```

```
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:getVpcOrigin",
        "cloudfront:listAnycastIpLists",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listConflictingAliases",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByAnycastIpListId",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByVpcOriginId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listKeyValueStores",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudfront:listVpcOrigins",
        "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:getMetricWidgetImage",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
        "cloudwatch:listMetricStreams",
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
        "codebuild:batchGetBuildBatches",
        "codebuild:batchGetBuilds",
        "codebuild:batchGetFleets",
```

```
            "codebuild:batchGetProjects",
            "codebuild:listBuildBatches",
            "codebuild:listBuildBatchesForProject",
            "codebuild:listBuilds",
            "codebuild:listBuildsForProject",
            "codebuild:listCuratedEnvironmentImages",
            "codebuild:listFleets",
            "codebuild:listProjects",
            "codebuild:listSourceCredentials",
            "codecommit:batchGetRepositories",
            "codecommit:getBranch",
            "codecommit:getRepository",
            "codecommit:getRepositoryTriggers",
            "codecommit:listBranches",
            "codecommit:listRepositories",
            "codeconnections:getConnection",
            "codeconnections:getHost",
            "codeconnections:getRepositoryLink",
            "codeconnections:getRepositorySyncStatus",
            "codeconnections:getResourceSyncStatus",
            "codeconnections:getSyncBlockerSummary",
            "codeconnections:getSyncConfiguration",
            "codeconnections:listConnections",
            "codeconnections:listHosts",
            "codeconnections:listRepositoryLinks",
            "codeconnections:listRepositorySyncDefinitions",
            "codeconnections:listSyncConfigurations",
            "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:listRuleExecutions",
            "codepipeline:listWebhooks",
            "codestar-connections:getConnection",
            "codestar-connections:getHost",
            "codestar-connections:listConnections",
            "codestar-connections:listHosts",
            "codestar:describeProject",
            "codestar:listProjects",
            "codestar:listResources",
            "codestar:listTeamMembers",
            "codestar:listUserProfiles",
            "cognito-identity:describeIdentity",
            "cognito-identity:describeIdentityPool",
            "cognito-identity:getIdentityPoolAnalytics",
            "cognito-identity:getIdentityPoolDailyAnalytics",
            "cognito-identity:getIdentityPoolRoles",
            "cognito-identity:getIdentityProviderDailyAnalytics",
            "cognito-identity:listIdentities",
            "cognito-identity:listIdentityPools",
            "cognito-identity:lookupDeveloperIdentity",
            "cognito-idp:describeIdentityProvider",
            "cognito-idp:describeResourceServer",
            "cognito-idp:describeRiskConfiguration",
            "cognito-idp:describeUserImportJob",
            "cognito-idp:describeUserPool",
            "cognito-idp:describeUserPoolClient",
            "cognito-idp:describeUserPoolDomain",
            "cognito-idp:getCSVHeader",
            "cognito-idp:getGroup",
```

```
        "cognito-idp:getLogDeliveryConfiguration",
        "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:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getEnrollmentStatus",
        "compute-optimizer:getIdleRecommendations",
        "compute-optimizer:getRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:getRDSDatabaseRecommendations",
        "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",
        "config:selectAggregateResourceConfig",
        "config:selectResourceConfig",
        "connect:batchGetFlowAssociation",
        "connect:describeContact",
        "connect:describeContactFlow",
        "connect:describeInstance",
        "connect:describeInstanceAttribute",
        "connect:describePhoneNumber",
        "connect:describeQueue",
        "connect:describeQuickConnect",
        "connect:describeRoutingProfile",
        "connect:describeUser",
        "connect:describeUserHierarchyStructure",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:getMetricDataV2",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listInstanceAttributes",
        "connect:listPhoneNumbersV2",
        "connect:listQueueQuickConnects",
        "connect:listQueues",
        "connect:listQuickConnects",
        "connect:listRoutingProfileQueues",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listSecurityProfilePermissions",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
        "connect:searchQueues",
        "connect:searchRoutingProfiles",
        "connect:searchUsers",
```

```
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getHomeRegion",
        "controltower:getLandingZone",
        "controltower:getLandingZoneStatus",
        "controltower:listDirectoryGroups",
        "controltower:listEnabledControls",
        "controltower:listGuardrailsForTarget",
        "controltower:listGuardrailViolations",
        "controltower:listLandingZones",
        "controltower:listManagedAccounts",
        "controltower:listManagedAccountsForGuardrail",
        "controltower:listManagedAccountsForParent",
        "controltower:listManagedOrganizationalUnits",
        "controltower:listManagedOrganizationalUnitsForGuardrail",
        "cost-optimization-hub:getPreferences",
        "cost-optimization-hub:getRecommendation",
        "cost-optimization-hub:listEnrollmentStatuses",
        "cost-optimization-hub:listRecommendations",
        "cost-optimization-hub:listRecommendationSummaries",
        "databrew:describeDataset",
        "databrew:describeJob",
        "databrew:describeProject",
        "databrew:describeRecipe",
        "databrew:listDatasets",
        "databrew:listJobRuns",
        "databrew:listJobs",
        "databrew:listProjects",
        "databrew:listRecipes",
        "databrew:listRecipeVersions",
        "databrew:listTagsForResource",
        "datapipeline:describeObjects",
        "datapipeline:describePipelines",
        "datapipeline:getPipelineDefinition",
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationAzureBlob",
        "datasync:describeLocationEfs",
```

```
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOntap",
        "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",
        "datazone:getAsset",
        "datazone:getAssetType",
        "datazone:getDataSource",
        "datazone:getDataSourceRun",
        "datazone:getDomain",
        "datazone:getEnvironment",
        "datazone:getEnvironmentBlueprint",
        "datazone:getEnvironmentBlueprintConfiguration",
        "datazone:getEnvironmentProfile",
        "datazone:getFormType",
        "datazone:getGlossary",
        "datazone:getGlossaryTerm",
        "datazone:getGroupProfile",
        "datazone:getListing",
        "datazone:getMetadataGenerationRun",
        "datazone:getProject",
        "datazone:getSubscription",
        "datazone:getSubscriptionGrant",
        "datazone:getSubscriptionRequestDetails",
        "datazone:getSubscriptionTarget",
        "datazone:getUserProfile",
        "datazone:listAssetRevisions",
        "datazone:listDataSourceRunActivities",
        "datazone:listDataSourceRuns",
        "datazone:listDataSources",
        "datazone:listDomains",
        "datazone:listEnvironmentBlueprintConfigurations",
        "datazone:listEnvironmentBlueprints",
        "datazone:listEnvironmentProfiles",
```

```
        "datazone:listEnvironments",
        "datazone:listMetadataGenerationRuns",
        "datazone:listProjectMemberships",
        "datazone:listProjects",
        "datazone:listSubscriptionGrants",
        "datazone:listSubscriptionRequests",
        "datazone:listSubscriptions",
        "datazone:listSubscriptionTargets",
        "datazone:searchGroupProfiles",
        "datazone:searchUserProfiles",
        "dax:describeClusters",
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
        "deadline:listAvailableMeteredProducts",
        "deadline:listBudgets",
        "deadline:listFarmMembers",
        "deadline:listFarms",
        "deadline:listFleetMembers",
        "deadline:listFleets",
        "deadline:listJobMembers",
        "deadline:listJobs",
        "deadline:listLicenseEndpoints",
        "deadline:listMeteredProducts",
        "deadline:listMonitors",
        "deadline:listQueueEnvironments",
        "deadline:listQueueFleetAssociations",
        "deadline:listQueueMembers",
        "deadline:listQueues",
        "deadline:listStorageProfiles",
        "deadline:listWorkers",
        "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",
        "directconnect:listVirtualInterfaceTestHistory",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
```

```
            "dms:describeConnections",
            "dms:describeEndpoints",
            "dms:describeEndpointSettings",
            "dms:describeEndpointTypes",
            "dms:describeEventCategories",
            "dms:describeEvents",
            "dms:describeEventSubscriptions",
            "dms:describeFleetAdvisorCollectors",
            "dms:describeFleetAdvisorDatabases",
            "dms:describeFleetAdvisorLsaAnalysis",
            "dms:describeFleetAdvisorSchemaObjectSummary",
            "dms:describeFleetAdvisorSchemas",
            "dms:describeOrderableReplicationInstances",
            "dms:describePendingMaintenanceActions",
            "dms:describeRefreshSchemasStatus",
            "dms:describeReplicationInstances",
            "dms:describeReplicationInstanceTaskLogs",
            "dms:describeReplicationSubnetGroups",
            "dms:describeReplicationTaskAssessmentResults",
            "dms:describeReplicationTaskAssessmentRuns",
            "dms:describeReplicationTaskIndividualAssessments",
            "dms:describeReplicationTasks",
            "dms:describeSchemas",
            "dms:describeTableStatistics",
            "docdb-elastic:getCluster",
            "docdb-elastic:getClusterSnapshot",
            "docdb-elastic:listClusters",
            "docdb-elastic:listClusterSnapshots",
            "drs:describeJobLogItems",
            "drs:describeJobs",
            "drs:describeLaunchConfigurationTemplates",
            "drs:describeRecoveryInstances",
            "drs:describeRecoverySnapshots",
            "drs:describeReplicationConfigurationTemplates",
            "drs:describeSourceNetworks",
            "drs:describeSourceServers",
            "drs:getLaunchConfiguration",
            "drs:getReplicationConfiguration",
            "drs:listExtensibleSourceServers",
            "drs:listLaunchActions",
            "drs:listStagingAccounts",
            "ds:describeClientAuthenticationSettings",
            "ds:describeConditionalForwarders",
            "ds:describeDirectories",
```

```
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeHybridADUpdate",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dsql:getCluster",
        "dsql:getVpcEndpointServiceName",
        "dsql:listClusters",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeGlobalTableSettings",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTableReplicaAutoScaling",
        "dynamodb:describeTimeToLive",
        "dynamodb:getResourcePolicy",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ebs:listChangedBlocks",
        "ebs:listSnapshotBlocks",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
```

```
            "ec2:describeAvailabilityZones",
            "ec2:describeBundleTasks",
            "ec2:describeByoipCidrs",
            "ec2:describeCapacityBlockOfferings",
            "ec2:describeCapacityManagerDataExports",
            "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:describeInstanceConnectEndpoints",
            "ec2:describeInstanceCreditSpecifications",
            "ec2:describeInstanceEventNotificationAttributes",
            "ec2:describeInstanceEventWindows",
```

```
            "ec2:describeInstances",
            "ec2:describeInstanceStatus",
            "ec2:describeInstanceTypeOfferings",
            "ec2:describeInstanceTypes",
            "ec2:describeInternetGateways",
            "ec2:describeIpamByoasn",
            "ec2:describeIpamExternalResourceVerificationTokens",
            "ec2:describeIpamPools",
            "ec2:describeIpamResourceDiscoveries",
            "ec2:describeIpamResourceDiscoveryAssociations",
            "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:describeNetworkInsightsAccessScopeAnalyses",
            "ec2:describeNetworkInsightsAccessScopes",
            "ec2:describeNetworkInsightsAnalyses",
            "ec2:describeNetworkInsightsPaths",
            "ec2:describeNetworkInterfaceAttribute",
            "ec2:describeNetworkInterfaces",
            "ec2:describeOutpostLags",
            "ec2:describePlacementGroups",
            "ec2:describePrefixLists",
            "ec2:describePrincipalIdFormat",
            "ec2:describePublicIpv4Pools",
            "ec2:describeRegions",
            "ec2:describeReplaceRootVolumeTasks",
            "ec2:describeReservedInstances",
            "ec2:describeReservedInstancesListings",
            "ec2:describeReservedInstancesModifications",
            "ec2:describeReservedInstancesOfferings",
            "ec2:describeRouteServerEndpoints",
```

```
        "ec2:describeRouteServerPeers",
        "ec2:describeRouteServers",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeServiceLinkVirtualInterfaces",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilterRules",
        "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:describeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
```

```
        "ec2:describeVpcAttribute",
        "ec2:describeVpcBlockPublicAccessExclusions",
        "ec2:describeVpcBlockPublicAccessOptions",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointAssociations",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedEnclaveCertificateIamRoles",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityManagerAttributes",
        "ec2:getCapacityManagerMetricData",
        "ec2:getCapacityManagerMetricDimensions",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getImageBlockPublicAccessState",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamDiscoveredAccounts",
        "ec2:getIpamDiscoveredPublicAddresses",
        "ec2:getIpamDiscoveredResourceCidrs",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getNetworkInsightsAccessScopeContent",
        "ec2:getReservedInstancesExchangeQuote",
```

```
            "ec2:getRouteServerAssociations",
            "ec2:getRouteServerPropagations",
            "ec2:getRouteServerRoutingDatabase",
            "ec2:getSerialConsoleAccessStatus",
            "ec2:getSpotPlacementScores",
            "ec2:getSubnetCidrReservations",
            "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:describeImageReplicationStatus",
            "ecr:describeImages",
            "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:describeServiceDeployments",
            "ecs:describeServiceRevisions",
            "ecs:describeServices",
```

```
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServiceDeployments",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup2",
      "Action" : [
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeClusterVersions",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeInsight",
        "eks:describeNodegroup",
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
```

```
        "eks:listIdentityProviderConfigs",
        "eks:listInsights",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "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:describeApplications",
        "elasticbeanstalk:describeApplicationVersions",
        "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:describeConfigurationSettings",
        "elasticbeanstalk:validateConfigurationSettings",
```

```
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeBackupPolicy",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeReplicationConfigurations",
        "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",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describePersistentAppUI",
        "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",
        "elasticmapreduce:listSupportedInstanceTypes",
        "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:describeDomainHealth",
        "es:describeDomainNodes",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:getDomainMaintenanceStatus",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
```

```
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainMaintenances",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "evidently:getExperiment",
        "evidently:getFeature",
        "evidently:getLaunch",
        "evidently:getProject",
        "evidently:getSegment",
        "evidently:listExperiments",
        "evidently:listFeatures",
        "evidently:listLaunches",
        "evidently:listProjects",
```

```
        "evidently:listSegmentReferences",
        "evidently:listSegments",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fis:getAction",
        "fis:getExperiment",
        "fis:getExperimentTargetAccountConfiguration",
        "fis:getExperimentTemplate",
        "fis:getSafetyLever",
        "fis:getTargetAccountConfiguration",
        "fis:listActions",
        "fis:listExperimentResolvedTargets",
        "fis:listExperimentTargetAccountConfigurations",
        "fis:listExperiments",
        "fis:listExperimentTemplates",
        "fis:listTargetAccountConfigurations",
        "fms:getAdminAccount",
        "fms:getAdminScope",
        "fms:getAppsList",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
        "fms:getProtocolsList",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:getResourceSet",
        "fms:getThirdPartyFirewallAssociationStatus",
        "fms:getViolationDetails",
        "fms:listAdminAccountsForOrganization",
        "fms:listAdminsManagingAccount",
        "fms:listAppsLists",
        "fms:listComplianceStatus",
        "fms:listDiscoveredResources",
        "fms:listMemberAccounts",
        "fms:listProtocolsLists",
        "fms:listPolicies",
        "fms:listResourceSetResources",
        "fms:listResourceSets",
        "fms:listThirdPartyFirewallFirewallPolicies",
        "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",
        "freetier:getFreeTierUsage",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeS3AccessPointAttachments",
        "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",
        "geo:calculateRoute",
        "geo:calculateRouteMatrix",
        "geo:describeMap",
        "geo:describePlaceIndex",
        "geo:describeRouteCalculator",
        "geo:describeTracker",
        "geo:getMapGlyphs",
        "geo:getMapSprites",
        "geo:getMapStyleDescriptor",
        "geo:getMapTile",
        "geo:getPlace",
        "geo:listGeofenceCollections",
        "geo:listMaps",
        "geo:listPlaceIndexes",
        "geo:listRouteCalculators",
        "geo:listTrackerConsumers",
        "geo:searchPlaceIndexForPosition",
        "geo:searchPlaceIndexForSuggestions",
        "geo:searchPlaceIndexForText",
        "geo-maps:getStaticMap",
        "geo-maps:getTile",
        "geo-places:autocomplete",
        "geo-places:geocode",
        "geo-places:getPlace",
        "geo-places:reverseGeocode",
        "geo-places:searchNearby",
        "geo-places:searchText",
        "geo-places:suggest",
        "geo-routes:calculateIsolines",
        "geo-routes:calculateRouteMatrix",
        "geo-routes:calculateRoutes",
        "geo-routes:optimizeWaypoints",
        "geo-routes:snapToRoads",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
```

```
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeCrossAccountAttachment",
        "globalaccelerator:describeCustomRoutingAccelerator",
        "globalaccelerator:describeCustomRoutingAcceleratorAttributes",
        "globalaccelerator:describeCustomRoutingEndpointGroup",
        "globalaccelerator:describeCustomRoutingListener",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listByoipCidrs",
        "globalaccelerator:listCrossAccountAttachments",
        "globalaccelerator:listCrossAccountResourceAccounts",
        "globalaccelerator:listCrossAccountResources",
        "globalaccelerator:listCustomRoutingAccelerators",
        "globalaccelerator:listCustomRoutingEndpointGroups",
        "globalaccelerator:listCustomRoutingListeners",
        "globalaccelerator:listCustomRoutingPortMappings",
        "globalaccelerator:listCustomRoutingPortMappingsByDestination",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:batchGetTableOptimizer",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalog",
        "glue:getCatalogImportStatus",
        "glue:getCatalogs",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
```

```
        "glue:getColumnStatisticsTaskRun",
        "glue:getColumnStatisticsTaskRuns",
        "glue:getCompletion",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataCatalogEncryptionSettings",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "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:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSecurityConfiguration",
        "glue:getSecurityConfigurations",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableOptimizer",
        "glue:getTableVersion",
```

```
            "glue:getTables",
            "glue:getTableVersions",
            "glue:getTrigger",
            "glue:getTriggers",
            "glue:getUserDefinedFunction",
            "glue:getUserDefinedFunctions",
            "glue:getWorkflow",
            "glue:getWorkflowRun",
            "glue:getWorkflowRuns",
            "glue:listColumnStatisticsTaskRuns",
            "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:listTableOptimizerRuns",
            "glue:listTriggers",
            "glue:querySchemaVersionMetadata",
            "glue:startCompletion",
            "grafana:describeWorkspace",
            "grafana:describeWorkspaceAuthentication",
            "grafana:listPermissions",
            "grafana:listVersions",
            "grafana:listWorkspaces",
            "greengrass:describeComponent",
            "greengrass:getComponent",
            "greengrass:getConnectivityInfo",
            "greengrass:getCoreDefinition",
            "greengrass:getCoreDefinitionVersion",
            "greengrass:getCoreDevice",
            "greengrass:getDeployment",
            "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:listClientDevicesAssociatedWithCoreDevice",
        "greengrass:listComponents",
        "greengrass:listComponentVersions",
        "greengrass:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listCoreDevices",
        "greengrass:listDeployments",
        "greengrass:listEffectiveDeployments",
        "greengrass:listInstalledComponents",
        "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:describeMalwareScans",
        "guardduty:describePublishingDestination",
        "guardduty:getCoverageStatistics",
        "guardduty:getDetector",
        "guardduty:getFilter",
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMalwareScanSettings",
        "guardduty:getMasterAccount",
        "guardduty:getMemberDetectors",
        "guardduty:getMembers",
        "guardduty:getOrganizationStatistics",
```

```
        "guardduty:getRemainingFreeTrialDays",
        "guardduty:getThreatIntelSet",
        "guardduty:listCoverage",
        "guardduty:listDetectors",
        "guardduty:listFilters",
        "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:getMFADevice",
        "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:listServiceSpecificCredentials",
            "iam:listSigningCertificates",
            "iam:listSSHPublicKeys",
            "iam:listUserPolicies",
            "iam:listUsers",
            "iam:listVirtualMFADevices",
            "iam:simulateCustomPolicy",
            "iam:simulatePrincipalPolicy",
            "identitystore:describeGroup",
            "identitystore:describeGroupMembership",
            "identitystore:getGroupId",
            "identitystore:getGroupMembershipId",
            "identitystore:getUserId",
            "identitystore:isMemberInGroups",
            "identitystore:listGroupMemberships",
            "identitystore:listGroupMembershipsForMember",
            "identitystore:listGroups",
            "imagebuilder:getComponent",
            "imagebuilder:getComponentPolicy",
            "imagebuilder:getContainerRecipe",
            "imagebuilder:getContainerRecipePolicy",
            "imagebuilder:getDistributionConfiguration",
            "imagebuilder:getImage",
            "imagebuilder:getImagePipeline",
```

```
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflow",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listTagsForResource",
        "imagebuilder:listWorkflowBuildVersions",
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflows",
        "imagebuilder:listWaitingWorkflowSteps",
        "imagebuilder:listWorkflowStepExecutions",
        "inspector-scan:scanSbom",
        "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:getConfiguration",
        "inspector2:getDelegatedAdminAccount",
        "inspector2:getEc2DeepInspectionConfiguration",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCisScanConfigurations",
        "inspector2:listCisScanResultsAggregatedByChecks",
        "inspector2:listCisScanResultsAggregatedByTargetResource",
        "inspector2:listCisScans",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "internetmonitor:getHealthEvent",
        "internetmonitor:getMonitor",
        "internetmonitor:listHealthEvents",
        "internetmonitor:listMonitors",
        "invoicing:batchGetInvoiceProfile",
        "invoicing:listInvoiceSummaries",
        "invoicing:listInvoiceUnits",
        "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:listCommandExecutions",
        "iot:listCommands",
        "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:getEncryptionConfiguration",
        "iotfleetwise:getFleet",
        "iotfleetwise:getLoggingOptions",
```

```
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getRegisterAccountStatus",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getStateTemplate",
        "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:listStateTemplates",
        "iotfleetwise:listVehicles",
        "iotfleetwise:listVehiclesInFleet",
        "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:getSyncJob",
        "iottwinmaker:getWorkspace",
```

```
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
        "iottwinmaker:listScenes",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
```

```
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeDataSource",
        "kendra:describeFaq",
        "kendra:describeIndex",
        "kendra:listDataSources",
        "kendra:listFaqs",
        "kendra:listIndices",
        "kinesis:describeStream",
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
        "kinesis:listShards",
        "kinesis:listStreamConsumers",
        "kinesis:listStreams",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationOperation",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplicationOperations",
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisanalytics:listApplicationVersions",
        "kinesisvideo:describeImageGenerationConfiguration",
        "kinesisvideo:describeEdgeConfiguration",
        "kinesisvideo:describeMappedResourceConfiguration",
        "kinesisvideo:describeMediaStorageConfiguration",
```

```
        "kinesisvideo:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
        "kinesisvideo:listEdgeAgentConfigurations",
        "kinesisvideo:listStreams",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
        "lakeformation:describeLakeFormationIdentityCenterConfiguration",
        "lakeformation:describeResource",
        "lakeformation:describeTransaction",
        "lakeformation:getDataLakePrincipal",
        "lakeformation:getDataLakeSettings",
        "lakeformation:getEffectivePermissionsForPath",
        "lakeformation:getLFTag",
        "lakeformation:getLFTagExpression",
        "lakeformation:getQueryState",
        "lakeformation:getQueryStatistics",
        "lakeformation:getResourceLFTags",
        "lakeformation:listLFTagExpressions",
        "lakeformation:listLFTags",
        "lakeformation:listLakeFormationOptIns",
        "lakeformation:listPermissions",
        "lakeformation:listResources",
        "lakeformation:searchDatabasesByLFTags",
        "lakeformation:searchTablesByLFTags",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
```

```
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionRecursionConfig",
        "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:listTags",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listDeploymentEvents",
        "launchwizard:listDeployments",
        "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:getGrant",
        "license-manager:getLicense",
        "license-manager:getLicenseConfiguration",
        "license-manager:getLicenseConversionTask",
        "license-manager:getLicenseManagerReportGenerator",
        "license-manager:getLicenseUsage",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
        "license-manager:listDistributedGrants",
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseConversionTasks",
        "license-manager:listLicenseManagerReportGenerators",
        "license-manager:listLicenses",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listLicenseVersions",
        "license-manager:listReceivedGrants",
        "license-manager:listReceivedGrantsForOrganization",
        "license-manager:listReceivedLicenses",
        "license-manager:listReceivedLicensesForOrganization",
        "license-manager:listResourceInventory",
        "license-manager:listTokens",
        "license-manager:listUsageForLicenseConfiguration",
        "license-manager-linux-subscriptions:getRegisteredSubscriptionProvider",
```

```
        "license-manager-linux-subscriptions:getServiceSettings",
        "license-manager-linux-subscriptions:listLinuxSubscriptionInstances",
        "license-manager-linux-subscriptions:listLinuxSubscriptions",
        "license-manager-linux-subscriptions:listRegisteredSubscriptionProviders",
        "license-manager-user-subscriptions:listIdentityProviders",
        "license-manager-user-subscriptions:listInstances",
        "license-manager-user-subscriptions:listLicenseServerEndpoints",
        "license-manager-user-subscriptions:listProductSubscriptions",
        "license-manager-user-subscriptions:listUserAssociations",
        "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:describeFieldIndexes",
        "logs:describeIndexPolicies",
        "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:getIntegration",
        "logs:getLogAnomalyDetector",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:getTransformer",
        "logs:listAnomalies",
        "logs:listIntegrations",
        "logs:listLogAnomalyDetectors",
        "logs:listLogDeliveries",
        "logs:listLogGroupsForQuery",
```

```
        "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",
        "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",
        "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:getCloudWatchAlarmTemplate",
        "medialive:getCloudWatchAlarmTemplateGroup",
        "medialive:getEventBridgeRuleTemplate",
        "medialive:getEventBridgeRuleTemplateGroup",
        "medialive:getSignalMap",
        "medialive:listChannels",
        "medialive:listCloudWatchAlarmTemplateGroups",
        "medialive:listCloudWatchAlarmTemplates",
        "medialive:listEventBridgeRuleTemplateGroups",
```

```
        "medialive:listEventBridgeRuleTemplates",
        "medialive:listInputDevices",
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "medialive:listSignalMaps",
        "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",
        "memorydb:describeReservedNodesOfferings",
        "memorydb:listAllowedNodeTypeUpdates",
        "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:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "mobiletargeting:phoneNumberValidate",
        "mpa:getApprovalTeam",
        "mpa:getSession",
        "mpa:listApprovalTeams",
        "mq:describeBrokerInstanceOptions",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeFlowOperation",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeResourcePolicy",
        "network-firewall:describeRuleGroup",
```

```
            "network-firewall:describeRuleGroupMetadata",
            "network-firewall:describeTlsInspectionConfiguration",
            "network-firewall:describeVpcEndpointAssociation",
            "network-firewall:listAnalysisReports",
            "network-firewall:listFirewallPolicies",
            "network-firewall:listFirewalls",
            "network-firewall:listFlowOperationResults",
            "network-firewall:listFlowOperations",
            "network-firewall:listRuleGroups",
            "network-firewall:listTlsInspectionConfigurations",
            "network-firewall:listVpcEndpointAssociations",
            "networkflowmonitor:getMonitor",
            "networkflowmonitor:getScope",
            "networkflowmonitor:listMonitors",
            "networkflowmonitor:listScopes",
            "networkmanager:describeGlobalNetworks",
            "networkmanager:getConnectAttachment",
            "networkmanager:getConnections",
            "networkmanager:getConnectPeer",
            "networkmanager:getConnectPeerAssociations",
            "networkmanager:getCoreNetwork",
            "networkmanager:getCoreNetworkChangeEvents",
            "networkmanager:getCoreNetworkChangeSet",
            "networkmanager:getCoreNetworkPolicy",
            "networkmanager:getCustomerGatewayAssociations",
            "networkmanager:getDevices",
            "networkmanager:getDirectConnectGatewayAttachment",
            "networkmanager:getLinkAssociations",
            "networkmanager:getLinks",
            "networkmanager:getNetworkResourceCounts",
            "networkmanager:getNetworkResourceRelationships",
            "networkmanager:getNetworkResources",
            "networkmanager:getNetworkRoutes",
            "networkmanager:getNetworkTelemetry",
            "networkmanager:getResourcePolicy",
            "networkmanager:getRouteAnalysis",
            "networkmanager:getSites",
            "networkmanager:getSiteToSiteVpnAttachment",
            "networkmanager:getTransitGatewayConnectPeerAssociations",
            "networkmanager:getTransitGatewayPeering",
            "networkmanager:getTransitGatewayRegistrations",
            "networkmanager:getTransitGatewayRouteTableAttachment",
            "networkmanager:getVpcAttachment",
            "networkmanager:listAttachments",
```

```
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
        "networkmanager:listCoreNetworks",
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "networkmonitor:getMonitor",
        "networkmonitor:getProbe",
        "networkmonitor:listMonitors",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "notifications:getEventRule",
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
        "notifications:listNotificationHubs"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup3",
      "Action" : [
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "observabilityadmin:getTelemetryEvaluationStatus",
        "observabilityadmin:getTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:listResourceTelemetry",
        "observabilityadmin:listResourceTelemetryForOrganization",
        "odb:getCloudAutonomousVmCluster",
        "odb:getCloudVmCluster",
        "odb:getOciOnboardingStatus",
        "odb:getOdbNetwork",
        "odb:getOdbPeeringConnection",
        "odb:listCloudAutonomousVmClusters",
```

```
        "odb:listCloudVmClusters",
        "odb:listOdbNetworks",
        "odb:listOdbPeeringConnections",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getAnnotationStoreVersion",
        "omics:getReadSetActivationJob",
        "omics:getReadSetExportJob",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunCache",
        "omics:getRunGroup",
        "omics:getRunTask",
        "omics:getSequenceStore",
        "omics:getShare",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:getWorkflowVersion",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listAnnotationStoreVersions",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetActivationJobs",
        "omics:listReadSetExportJobs",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferences",
        "omics:listReferenceStores",
        "omics:listRunCaches",
        "omics:listRunGroups",
        "omics:listRuns",
        "omics:listRunTasks",
        "omics:listSequenceStores",
        "omics:listShares",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
```

```
            "omics:listWorkflows",
            "omics:listWorkflowVersions",
            "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:describeAccount",
            "organizations:describeCreateAccountStatus",
            "organizations:describeEffectivePolicy",
            "organizations:describeHandshake",
            "organizations:describeOrganization",
            "organizations:describeOrganizationalUnit",
            "organizations:describePolicy",
            "organizations:describeResourcePolicy",
            "organizations:listAccounts",
            "organizations:listAccountsForParent",
            "organizations:listAWSServiceAccessForOrganization",
            "organizations:listChildren",
            "organizations:listCreateAccountStatus",
            "organizations:listDelegatedAdministrators",
            "organizations:listDelegatedServicesForAccount",
```

```
        "organizations:listHandshakesForAccount",
        "organizations:listHandshakesForOrganization",
        "organizations:listOrganizationalUnitsForParent",
        "organizations:listParents",
        "organizations:listPolicies",
        "organizations:listPoliciesForTarget",
        "organizations:listRoots",
        "organizations:listTagsForResource",
        "organizations:listTargetsForPolicy",
        "osis:getPipeline",
        "osis:getPipelineBlueprint",
        "osis:getPipelineChangeProgress",
        "osis:listPipelineBlueprints",
        "osis:listPipelines",
        "osis:validatePipeline",
        "outposts:getCapacityTask",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getOutpostSupportedInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listAssetInstances",
        "outposts:listBlockingInstancesForCapacityTask",
        "outposts:listCapacityTasks",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "payment-cryptography:getAlias",
        "payment-cryptography:getKey",
        "payment-cryptography:listAliases",
        "payment-cryptography:listKeys",
        "pcs:getCluster",
        "pcs:getComputeNodeGroup",
        "pcs:getQueue",
        "pcs:listClusters",
        "pcs:listComputeNodeGroups",
        "pcs:listQueues",
        "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:listNetworkResources",
        "private-networks:listNetworks",
```

```
        "qbusiness:getApplication",
        "qbusiness:getDataSource",
        "qbusiness:getIndex",
        "qbusiness:getRetriever",
        "qbusiness:getWebExperience",
        "qbusiness:listApplications",
        "qbusiness:listDataSources",
        "qbusiness:listDataSourceSyncJobs",
        "qbusiness:listIndices",
        "qbusiness:listRetrievers",
        "qbusiness:listWebExperiences",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
```

```
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboards",
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
```

```
            "rds:describeCertificates",
            "rds:describeDBClusterAutomatedBackups",
            "rds:describeDBClusterBacktracks",
            "rds:describeDBClusterEndpoints",
            "rds:describeDBClusterParameterGroups",
            "rds:describeDBClusterParameters",
            "rds:describeDBClusters",
            "rds:describeDBClusterSnapshots",
            "rds:describeDBClusterSnapshotAttributes",
            "rds:describeDBEngineVersions",
            "rds:describeDBInstanceAutomatedBackups",
            "rds:describeDBInstances",
            "rds:describeDBLogFiles",
            "rds:describeDBMajorEngineVersions",
            "rds:describeDBParameterGroups",
            "rds:describeDBParameters",
            "rds:describeDBProxies",
            "rds:describeDBProxyEndpoints",
            "rds:describeDBProxyTargetGroups",
            "rds:describeDBProxyTargets",
            "rds:describeDBRecommendations",
            "rds:describeDBSecurityGroups",
            "rds:describeDBShardGroups",
            "rds:describeDBSnapshotAttributes",
            "rds:describeDBSnapshots",
            "rds:describeDBSnapshotTenantDatabases",
            "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:describeTenantDatabases",
            "rds:describeValidDBInstanceModifications",
```

```
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getCustomDomainAssociation",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getScheduledAction",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listCustomDomainAssociations",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshotCopyConfigurations",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterDbRevisions",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterTracks",
        "redshift:describeClusterVersions",
        "redshift:describeCustomDomainAssociations",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEndpointAccess",
        "redshift:describeEndpointAuthorization",
        "redshift:describeEventCategories",
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeInboundIntegrations",
        "redshift:describeLoggingStatus",
```

```
        "redshift:describeNodeConfigurationOptions",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeRedshiftIdcApplications",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeSnapshotSchedules",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift:describeUsageLimits",
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resiliencehub:describeApp",
        "resiliencehub:describeAppAssessment",
        "resiliencehub:describeAppVersion",
        "resiliencehub:describeAppVersionAppComponent",
        "resiliencehub:describeAppVersionResource",
        "resiliencehub:describeAppVersionResourcesResolutionStatus",
        "resiliencehub:describeAppVersionTemplate",
        "resiliencehub:describeDraftAppVersionResourcesImportStatus",
        "resiliencehub:describeResiliencyPolicy",
        "resiliencehub:describeResourceGroupingRecommendationTask",
        "resiliencehub:listAlarmRecommendations",
        "resiliencehub:listAppAssessmentComplianceDrifts",
        "resiliencehub:listAppAssessmentResourceDrifts",
        "resiliencehub:listAppAssessments",
        "resiliencehub:listAppComponentCompliances",
        "resiliencehub:listAppComponentRecommendations",
        "resiliencehub:listAppInputSources",
        "resiliencehub:listApps",
        "resiliencehub:listAppVersionAppComponents",
        "resiliencehub:listAppVersionResourceMappings",
        "resiliencehub:listAppVersionResources",
        "resiliencehub:listAppVersions",
        "resiliencehub:listRecommendationTemplates",
        "resiliencehub:listResiliencyPolicies",
        "resiliencehub:listResourceGroupingRecommendations",
        "resiliencehub:listSopRecommendations",
        "resiliencehub:listSuggestedResiliencyPolicies",
        "resiliencehub:listTestRecommendations",
        "resiliencehub:listUnsupportedAppVersionResources",
        "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",
        "rolesanywhere:getProfile",
        "rolesanywhere:getTrustAnchor",
        "rolesanywhere:listProfiles",
        "rolesanywhere:listTrustAnchors",
        "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",
        "route53profiles:getProfile",
        "route53profiles:getProfileAssociation",
        "route53profiles:getProfileResourceAssociation",
        "route53profiles:listProfileAssociations",
        "route53profiles:listProfileResourceAssociations",
        "route53profiles:listProfiles",
        "route53profiles:listTagsForResource",
        "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-outposts:listEndpoints",
        "s3-outposts:listOutpostsWithS3",
```

```
        "s3-outposts:listRegionalBuckets",
        "s3-outposts:listSharedEndpoints",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessGrant",
        "s3:getAccessGrantsInstance",
        "s3:getAccessGrantsInstanceResourcePolicy",
        "s3:getAccessGrantsLocation",
        "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:getObjectAcl",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
```

```
            "s3:getStorageLensConfiguration",
            "s3:listAccessGrants",
            "s3:listAccessGrantsInstances",
            "s3:listAccessGrantsLocations",
            "s3:listAccessPoints",
            "s3:listAccessPointsForObjectLambda",
            "s3:listAllMyBuckets",
            "s3:listBucket",
            "s3:listBucketMultipartUploads",
            "s3:listBucketVersions",
            "s3:listJobs",
            "s3:listMultipartUploadParts",
            "s3:listMultiRegionAccessPoints",
            "s3:listStorageLensConfigurations",
            "s3express:getBucketPolicy",
            "s3express:listAllMyDirectoryBuckets",
            "s3tables:getNamespace",
            "s3tables:getTable",
            "s3tables:getTableBucket",
            "s3tables:getTableBucketEncryption",
            "s3tables:getTableBucketMaintenanceConfiguration",
            "s3tables:getTableBucketPolicy",
            "s3tables:getTableEncryption",
            "s3tables:getTableMaintenanceConfiguration",
            "s3tables:getTableMaintenanceJobStatus",
            "s3tables:getTableMetadataLocation",
            "s3tables:getTablePolicy",
            "s3tables:listNamespaces",
            "s3tables:listTableBuckets",
            "s3tables:listTables",
            "s3vectors:getIndex",
            "s3vectors:getVectorBucket",
            "s3vectors:getVectorBucketPolicy",
            "s3vectors:listIndexes",
            "s3vectors:listVectorBuckets",
            "sagemaker:describeAction",
            "sagemaker:describeAlgorithm",
            "sagemaker:describeApp",
            "sagemaker:describeAppImageConfig",
            "sagemaker:describeArtifact",
            "sagemaker:describeAutoMLJob",
            "sagemaker:describeCluster",
            "sagemaker:describeClusterNode",
            "sagemaker:describeCodeRepository",
```

```
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeMlflowTrackingServer",
        "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:describePartnerApp",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
```

```
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContents",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImages",
        "sagemaker:listImageVersions",
        "sagemaker:listInferenceComponents",
```

```
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listMlflowTrackingServers",
        "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:listPartnerApps",
        "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:batchGetAutomationRules",
            "securityhub:batchGetConfigurationPolicyAssociations",
            "securityhub:describeHub",
            "securityhub:describeOrganizationConfiguration",
            "securityhub:getConfigurationPolicy",
            "securityhub:getConfigurationPolicyAssociation",
            "securityhub:getEnabledStandards",
            "securityhub:getFindingAggregator",
            "securityhub:getFindingHistory",
            "securityhub:getFindings",
            "securityhub:getInsightResults",
            "securityhub:getInsights",
            "securityhub:getMasterAccount",
            "securityhub:getMembers",
            "securityhub:listAutomationRules",
            "securityhub:listConfigurationPolicies",
            "securityhub:listConfigurationPolicyAssociations",
            "securityhub:listEnabledProductsForImport",
            "securityhub:listFindingAggregators",
            "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:batchGetMetricData",
        "ses:describeActiveReceiptRuleSet",
```

```
            "ses:describeConfigurationSet",
            "ses:describeReceiptRule",
            "ses:describeReceiptRuleSet",
            "ses:getAccount",
            "ses:getAccountSendingEnabled",
            "ses:getAddonInstance",
            "ses:getAddonSubscription",
            "ses:getArchive",
            "ses:getArchiveExport",
            "ses:getArchiveSearch",
            "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:getIngressPoint",
            "ses:getMessageInsights",
            "ses:getRelay",
            "ses:getRuleSet",
            "ses:getTrafficPolicy",
            "ses:getSendQuota",
            "ses:getSendStatistics",
            "ses:listConfigurationSets",
            "ses:listAddonInstances",
            "ses:listAddonSubscriptions",
            "ses:listArchiveExports",
            "ses:listArchives",
            "ses:listArchiveSearches",
            "ses:listContactLists",
            "ses:listContacts",
            "ses:listCustomVerificationEmailTemplates",
```

```
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listIngressPoints",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRelays",
        "ses:listRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listTrafficPolicies",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeProtection",
        "shield:describeSubscription",
        "shield:listAttacks",
        "shield:listProtections",
        "signer:describeSigningJob",
        "signer:getRevocationStatus",
        "signer:getSigningPlatform",
        "signer:getSigningProfile",
        "signer:listProfilePermissions",
        "signer:listSigningJobs",
        "signer:listSigningPlatforms",
        "signer:listSigningProfiles",
        "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:listMessageMoveTasks",
        "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:batchGetIncidentFindings",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentFindings",
```

```
            "ssm-incidents:listIncidentRecords",
            "ssm-incidents:listRelatedItems",
            "ssm-incidents:listReplicationSets",
            "ssm-incidents:listResponsePlans",
            "ssm-incidents:listTimelineEvents",
            "ssm-quicksetup:getConfiguration",
            "ssm-quicksetup:getConfigurationManager",
            "ssm-quicksetup:getServiceSettings",
            "ssm-quicksetup:listConfigurationManagers",
            "ssm-quicksetup:listConfigurations",
            "ssm-quicksetup:listQuickSetupTypes",
            "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:describeInstanceProperties",
            "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:listDocumentMetadataHistory",
            "ssm:listDocuments",
            "ssm:listDocumentVersions",
            "ssm:listNodes",
            "ssm:listNodesSummary",
            "ssm:listOpsItemEvents",
            "ssm:listOpsItemRelatedItems",
            "ssm:listOpsMetadata",
            "ssm:listResourceComplianceSummaries",
            "ssm:listResourceDataSync",
```

```
        "ssm:listTagsForResource",
        "sso:describeApplication",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeAccountAssignmentCreationStatus",
        "sso:describeAccountAssignmentDeletionStatus",
        "sso:describeInstance",
        "sso:describeInstanceAccessControlAttributeConfiguration",
        "sso:describePermissionSet",
        "sso:describePermissionSetProvisioningStatus",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getInlinePolicyForPermissionSet",
        "sso:getManagedApplicationInstance",
        "sso:getPermissionsBoundaryForPermissionSet",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listAccountAssignmentCreationStatus",
        "sso:listAccountAssignmentDeletionStatus",
        "sso:listAccountAssignments",
        "sso:listAccountAssignmentsForPrincipal",
        "sso:listAccountsForProvisionedPermissionSet",
        "sso:listApplicationAssignmentsForPrincipal",
        "sso:listCustomerManagedPolicyReferencesInPermissionSet",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listManagedPoliciesInPermissionSet",
        "sso:listPermissionSetProvisioningStatus",
        "sso:listPermissionSets",
        "sso:listPermissionSetsProvisionedToAccount",
        "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",
            "sts:getCallerIdentity",
            "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",
        "tax:getTaxInheritance",
        "tax:getTaxRegistration",
        "thinclient:getDevice",
        "thinclient:getEnvironment",
        "thinclient:getSoftwareSet",
        "thinclient:listDevices",
        "thinclient:listEnvironments",
        "thinclient:listSoftwareSets",
        "timestream:describeAccountSettings",
        "timestream:describeBatchLoadTask",
        "timestream:describeDatabase",
        "timestream:describeEndpoints",
        "timestream:describeScheduledQuery",
        "timestream:describeTable",
        "timestream:listBatchLoadTasks",
        "timestream:listDatabases",
        "timestream:listScheduledQueries",
        "timestream:listTables",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
        "tnb:getSolFunctionInstance",
        "tnb:getSolFunctionPackage",
        "tnb:getSolNetworkInstance",
```

```
        "tnb:getSolNetworkOperation",
        "tnb:getSolNetworkPackage",
        "tnb:listSolFunctionInstances",
        "tnb:listSolFunctionPackages",
        "tnb:listSolNetworkInstances",
        "tnb:listSolNetworkOperations",
        "tnb:listSolNetworkPackages",
        "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:describeWebApp",
        "transfer:describeWebAppCustomization",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
        "transfer:listUsers",
        "transfer:listWebApps",
        "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:getResourceConfiguration",
        "vpc-lattice:getResourceGateway",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkResourceAssociation",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listResourceConfigurations",
        "vpc-lattice:listResourceGateways",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkResourceAssociations",
        "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:describeApplicationAssociations",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspaceSnapshots",
        "workspaces:describeWorkspacesConnectionStatus",
        "workspaces:describeWorkspacesPools",
        "workspaces:describeWorkspacesPoolSessions",
        "xray:getEncryptionConfig",
        "xray:getGroup",
        "xray:getGroups",
        "xray:getInsightImpactGraph",
        "xray:getSamplingRules",
        "xray:getSamplingStatisticSummaries",
        "xray:getSamplingTargets",
        "xray:getServiceGraph",
        "xray:getTimeSeriesServiceStatistics",
        "xray:getTraceGraph",
        "xray:listResourcePolicies"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
```

```
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSystemsManagerAccountDiscoveryServicePolicy

描述：授予 AWS Systems Manager (SSM) 許可來探索 AWS 帳戶 資訊。

`AWSSystemsManagerAccountDiscoveryServicePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 10 月 24 日 17：21 UTC
- 編輯時間：2022 年 10 月 17 日，UTC 20：25
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSSystemsManagerChangeManagementServicePolicy

描述：提供存取 AWS Systems Manager 變更管理架構所管理或使用 AWS 的資源。

`AWSSystemsManagerChangeManagementServicePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 7 日，22：21 UTC
- 編輯時間：2025 年 10 月 23 日，UTC 21：19
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation",
        "ssm:CreateOpsItem",
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:GetAutomationExecution",
        "ssm:GetCalendarState",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

描述：提供 AWS Systems Manager Quick Setup 啟用和設定 Config AWS 組態錄製的許可。

`AWSSystemsManagerEnableConfigRecordingExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSystemsManagerEnableConfigRecordingExecutionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：40 UTC
- 編輯時間：2024 年 6 月 26 日 09：40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-quick-setup-config-recording-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SNSTopicsListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultSNSTopicCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ConfigRecording-Default-Topic"
    },
    {
      "Sid" : "ConfigureAndStartConfigurationRecorderPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeDeliveryChannels",
        "config:PutConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:StartConfigurationRecorder"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetAndPassConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
        "arn:aws:iam::*:role/AWSServiceRoleForConfig"
      ]
    },
    {
      "Sid" : "CreateConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSystemsManagerEnableExplorerExecutionPolicy

描述：此政策會授予啟用 Explorer 的管理許可，這是 AWS Systems Manager 的功能。這包括更新相關 Systems Manager 服務設定的許可，以及為 Systems Manager 建立服務連結角色的許可。

`AWSSystemsManagerEnableExplorerExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 AWSSystemsManagerEnableExplorerExecutionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 6 月 26 日 09：42 UTC
- 編輯時間：2024 年 6 月 26 日 09：42 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSystemsManagerForSAPFullAccess

描述：提供 AWS Systems Manager for SAP 服務的完整存取權

AWSSystemsManagerForSAPFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSystemsManagerForSAPFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 17 日 02：11 UTC
- 編輯時間：2024 年 7 月 10 日 21：54 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsSsmForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
    {
      "Sid" : "AwsSsmForSapServiceRoleCreationPermission",
      "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"
        }
      }
    },
    {
      "Sid" : "Ec2StartStopPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSystemsManagerForSAPReadOnlyAccess

描述：提供 AWS Systems Manager for SAP 服務的唯讀存取權

AWSSystemsManagerForSAPReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSSystemsManagerForSAPReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 17 日 02：11 UTC
- 編輯時間：2022 年 11 月 17 日 02：11 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSystemsManagerJustInTimeAccessServicePolicy

描述：提供 AWS Systems Manager 即時管理或使用 AWS 的資源存取權。

AWSSystemsManagerJustInTimeAccessServicePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 4 月 21 日 20：07 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerJustInTimeAccessServicePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
        "ssm:CreateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemReplicationTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAutomationExecutionTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrieveDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : [
            "ManualApprovalPolicy",
            "AutoApprovalPolicy"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescriptions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeOpsItems",
        "ssm:DescribeSessions",
        "ssm:ListDocuments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListTagsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*"
      ]
    },
    {
      "Sid" : "AllowListSSMGUIConnections",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:ListConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetUserId"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribingEC2Tags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPublishingCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SSM/JustInTimeAccess"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSystemsManagerJustInTimeAccessTokenPolicy

描述：受管政策 AWSSystemsManagerJustInTimeAccessTokenPolicy 可讓 Systems Manager 產生用於just-in-time節點存取的存取權杖。

`AWSSystemsManagerJustInTimeAccessTokenPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSSystemsManagerJustInTimeAccessTokenPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 4 月 17 日，UTC 21：07
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenPolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "TerminateAndResumeSessionAndOpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssm:TerminateSession",
        "ssm:ResumeSession",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

描述：受管政策 AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 允許 Systems Manager 在啟動時，將範圍縮小的許可套用至just-in-time節點存取工作階段。

`AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 4 月 17 日 20：52 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
```

```
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

描述：此政策允許 Systems Manager 共用拒絕存取政策，以便從委派管理員帳戶just-in-time存取節點至成員帳戶，並將政策複寫至多個區域。

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 4 月 21 日，UTC 20：52
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:GetConfigurationManager",
        "cloudformation:ListStackSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ssm-quicksetup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QuickSetupSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-quicksetup.amazonaws.com/
AWSServiceRoleForSSMQuickSetup"
      ]
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SSMDocumentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:ListTagsForResource",
        "ssm:PutResourcePolicy",
        "ssm:DeleteResourcePolicy",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy"
        }
      }
    },
    {
      "Sid" : "SSMDocumentCreateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SSMDocumentUpdateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
```

```
        "ssm:UpdateDocumentMetadata",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
```

```
        }
      }
    },
    {
      "Sid" : "RAMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : "ram:TagResource",
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RAMModificationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "SSMJustInTimeNodeAccessManagedResourceShare",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSSystemsManagerNotificationsServicePolicy

描述：收集使用者相關資訊以進行Just-In-Time-Node-Access通知所需的許可。

`AWSSystemsManagerNotificationsServicePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 4 月 17 日 20：52 UTC
- 編輯時間：2025 年 4 月 17 日 20：52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerNotificationsServicePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroupMemberships",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUser",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIamActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSSystemsManagerOpsDataSyncServiceRolePolicy

描述：SSM Explorer 管理 OpsData 相關操作的 IAM 角色

`AWSSystemsManagerOpsDataSyncServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 4 月 26 日，UTC 20：42
- 編輯時間：2023 年 6 月 28 日 22：53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSThinkboxAssetServerPolicy

描述：此政策會授予 AWS 入口網站資產伺服器正常操作所需的必要許可。

AWSThinkboxAssetServerPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSThinkboxAssetServerPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 5 月 27 日 19：18 UTC
- 編輯時間：2020 年 5 月 27 日 19：18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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*"
      ]
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSThinkboxAWSPortalAdminPolicy

描述：此政策授予 AWS Thinkbox 的截止日期軟體對 AWS 入口網站管理所需的多項 AWS 服務的完整存取權。這包括在數種 EC2 資源類型上建立任意標籤的存取權。

`AWSThinkboxAWSPortalAdminPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSThinkboxAWSPortalAdminPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 5 月 27 日 19：41 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : {
        "ArnLike" : {
          "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" : {
        "Null" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : false
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
```

```
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*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/*",
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal10",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal11",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal12",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal13",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal14",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal15",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AWSThinkboxAWSPortal16",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal17",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-aws-portal-cache*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal18",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal19",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal20",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal21",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",
        "arn:aws:cloudformation:*:*:stack/Deadline*/*"
```

```
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal22",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:EstimateTemplateCost",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal23",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal24",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal25",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal26",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : [
            "rcs-tls-pw*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal27",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSThinkboxAWSPortalGatewayPolicy

描述：此政策會授予 AWS Portal Gateway 機器正常操作所需的必要許可。

AWSThinkboxAWSPortalGatewayPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSThinkboxAWSPortalGatewayPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 5 月 27 日，UTC 19：05
- 編輯時間：2020 年 6 月 30 日 16：02 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "dynamodb:Scan",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSThinkboxAWSPortalWorkerPolicy

描述：此政策授予 AWS 入口網站中的截止日期工作者正常操作所需的必要許可。

AWSThinkboxAWSPortalWorkerPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSThinkboxAWSPortalWorkerPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 5 月 27 日 19：15 UTC
- 編輯時間：2020 年 12 月 7 日 23：27 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSThinkboxDeadlineResourceTrackerAccessPolicy

描述：授予操作 AWS Thinkbox 的截止日期資源追蹤器所需的許可。這包括完整存取某些 EC2 動作，包括 DeleteFleets 和 CancelSpotFleetRequests。

`AWSThinkboxDeadlineResourceTrackerAccessPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSThinkboxDeadlineResourceTrackerAccessPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 5 月 27 日 19：25 UTC
- 編輯時間：2020 年 5 月 27 日 19：25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSThinkboxDeadlineResourceTrackerAdminPolicy

描述：授予建立、銷毀和管理 AWS Thinkbox 截止日期資源追蹤器所需的許可。

AWSThinkboxDeadlineResourceTrackerAdminPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSThinkboxDeadlineResourceTrackerAdminPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 5 月 27 日，UTC 19：29
- 編輯時間：2024 年 11 月 12 日 19：29 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker1",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "AWSThinkboxDeadlineResourceTracker2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker3",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker4",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker5",
```

```
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker6",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker7",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker8",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker9",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker12",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker13",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker14",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
```

```
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker15",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker16",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker-*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate-*.yaml"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker17",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
```

```
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

描述：授予 AWS Thinkbox 的截止日期 Spot 事件外掛程式所需的許可。這包括請求、修改和取消 Spot 機群的許可，以及有限的 PassRole 許可。

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSThinkboxDeadlineSpotEventPluginAdminPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 5 月 27 日 19：38 UTC
- 編輯時間：2020 年 5 月 27 日 19：38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

描述：授予執行 AWS Thinkbox Deadline Spot Event Plugin Worker 軟體的 EC2 執行個體所需的許可。

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 5 月 27 日，UTC 19：35
- 編輯時間：2020 年 12 月 7 日 23：31 UTC
- ARN: arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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*"
      ]
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTransferConsoleFullAccess

描述：提供透過 AWS 傳輸的完整存取權 AWS 管理主控台

`AWSTransferConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSTransferConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 14 日，UTC 19：33
- 編輯時間：2020 年 12 月 14 日，UTC 19：33
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTransferFullAccess

描述：提供 AWS Transfer Service 的完整存取權。

AWSTransferFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSTransferFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 12 月 14 日，UTC 19：37
- 編輯時間：2020 年 12 月 14 日 19：37 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTransferLoggingAccess

描述：允許 AWS 轉移完整存取權以建立日誌串流和群組，並將日誌事件放入您的帳戶

AWSTransferLoggingAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSTransferLoggingAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 1 月 14 日 15：32 UTC

- **編輯時間**：2019 年 1 月 14 日 15：32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTransferReadOnlyAccess

描述：提供 AWS Transfer 服務的唯讀存取權。

AWSTransferReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSTransferReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 8 月 27 日 17：54 UTC
- 編輯時間：2020 年 8 月 27 日 17：54 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTransformApplicationDeploymentPolicy

描述：透過建立和管理 AWS 資源，讓 AWS Transform 服務部署轉換的 .NET 應用程式。此政策授予許可，以佈建基礎設施、管理運算資源，以及設定跨各種 AWS 服務的部署設定。

`AWSTransformApplicationDeploymentPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `AWSTransformApplicationDeploymentPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 8 月 28 日 06：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationDeploymentPolicy`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSTransform*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:UpdateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringNotEquals" : {
          "aws:TagKeys" : [
            "Name",
            "CreatedBy",
            "ApplicationName",
            "TransformationType",
            "aws:cloudformation:stack-name",
            "aws:cloudformation:logical-id",
            "aws:cloudformation:stack-id"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      },
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/ami-amazon-linux-latest*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunRemoteScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:PutBucketTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-transform-deployment-bucket-*",
        "arn:aws:s3:::aws-transform-deployment-bucket-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedFor" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws-transform" : "*",
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ebs:id" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
```

```
            "Decrypt"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTransformApplicationECSDeploymentPolicy

描述：啟用 AWS 轉換以使用 Fargate 將應用程式部署至 Amazon Elastic Container Service (ECS)。它授予許可，以佈建、設定和管理在 ECS 上執行應用程式所需的基礎基礎設施。

AWSTransformApplicationECSDeploymentPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSTransformApplicationECSDeploymentPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 9 月 29 日，UTC 22：49
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/service-role/AWSTransformApplicationECSDeploymentPolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:CreateStack",
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
```

```
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RegisterTaskDefinition",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RunTask",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:ListTasks",
      "Resource" : "arn:aws:ecs:*:*:container-instance/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
```

```
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:DescribeTasks",
      "Resource" : "arn:aws:ecs:*:*:task/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
```

```
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateService",
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService"
      ],
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/AWSTransform*",
        "arn:aws:ecs:*:*:task-definition/AWSTransform*",
        "arn:aws:ecs:*:*:service/AWSTransform*",
        "arn:aws:ecs:*:*:task/AWSTransform*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:UntagResource",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/awstransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : [
            "ecr.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ecr:arn" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSTransformCustomExecuteTransformations

描述：提供在轉換自訂中執行 AWS 轉換的存取權。

AWSTransformCustomExecuteTransformations 是 AWS 受管政策。

使用此政策

您可以將 AWSTransformCustomExecuteTransformations 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 12 月 5 日 15：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomExecuteTransformations`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomExecuteTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:ExecuteTransformation",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSTransformCustomFullAccess

描述：提供 AWS 轉換自訂的完整存取權。

AWSTransformCustomFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSTransformCustomFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 12 月 5 日 15：19 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransformCustomFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomAllActions",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:*"
```

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTransformCustomManageTransformations

描述：啟用轉換資源的管理，並在轉換自訂中執行 AWS 轉換。

AWSTransformCustomManageTransformations 是 AWS 受管政策。

使用此政策

您可以將 AWSTransformCustomManageTransformations 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 12 月 5 日 15：49 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransformCustomManageTransformations

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomManageTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:CreateTransformationPackageUrl",
        "transform-custom:CompleteTransformationPackageUpload",
        "transform-custom:DeleteTransformationPackage",
        "transform-custom:GetTransformationPackageUrl",
        "transform-custom:ListTransformationPackageMetadata",
        "transform-custom:ExecuteTransformation",
        "transform-custom:ListKnowledgeItems",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:DeleteKnowledgeItem",
        "transform-custom:UpdateKnowledgeItemConfiguration",
        "transform-custom:UpdateKnowledgeItemStatus",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign",
        "transform-custom:ListTagsForResource",
        "transform-custom:TagResource",
        "transform-custom:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTransformSecretsManagerConnectorPolicy

描述：讓 AWS Transform 服務讀取與指定 KMS 金鑰相關聯的指定 SecretsManager Secret。此政策授予讀取指定秘密值的許可，並解密秘密已加密

AWSTransformSecretsManagerConnectorPolicy 是 AWS 受管政策。

使用此政策

您可以將 AWSTransformSecretsManagerConnectorPolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2026 年 3 月 4 日 21：12 UTC
- 編輯時間：2026 年 3 月 4 日 21：12 UTC
- ARN: arn:aws:iam::aws:policy/AWSTransformSecretsManagerConnectorPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadSecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:${aws:PrincipalTag/SecretId}",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DecryptWithCustomerProvidedKMSKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KMSKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:
${aws:RequestedRegion}:${aws:PrincipalAccount}:secret:${aws:PrincipalTag/SecretId}",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeKMSKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTrustedAdvisorPriorityFullAccess

描述：提供 AWS Trusted Advisor Priority 的完整存取權。此政策也允許使用者新增 Trusted Advisor 做為 AWS Organizations 的受信任服務，並指定 Trusted Advisor Priority 的委派管理員帳戶。

`AWSTrustedAdvisorPriorityFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSTrustedAdvisorPriorityFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 8 月 16 日 16：08 UTC
- 編輯時間：2022 年 8 月 16 日 16：08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTrustedAdvisorPriorityReadOnlyAccess

描述：提供 AWS 對 Trusted Advisor Priority 的唯讀存取權。這包括檢視委派管理員帳戶的許可。

`AWSTrustedAdvisorPriorityReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSTrustedAdvisorPriorityReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 8 月 16 日 16：35 UTC

- **編輯時間**：2022 年 8 月 16 日 16：35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTrustedAdvisorReportingServiceRolePolicy

描述：Trusted Advisor 多帳戶報告的服務政策

AWSTrustedAdvisorReportingServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 19 日 17：41 UTC
- 編輯時間：2023 年 2 月 28 日 23：23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSTrustedAdvisorServiceRolePolicy

描述：存取 AWS Trusted Advisor Service，以協助降低成本、提高效能並改善 AWS 環境的安全性。

`AWSTrustedAdvisorServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 2 月 22 日，UTC 21：24
- 編輯時間：2024 年 10 月 30 日 16：52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
```

```
        "cloudwatch:ListMetrics",
        "dax:DescribeClusters",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:GetManagedPrefixListEntries",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "iam:ListSAMLProviders",
        "kinesis:DescribeLimits",
```

```
        "kafka:DescribeClusterV2",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "network-firewall:ListFirewalls",
        "network-firewall:DescribeFirewall",
        "outposts:ListAssets",
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
```

```
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSUserAttributeCostAllocationPolicy

描述：針對客戶已選擇加入的使用者屬性，從 AWS IAM Identity Center 提供使用者屬性的唯讀存取權。

`AWSUserAttributeCostAllocationPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 12 月 15 日 16：34 UTC
- 編輯時間：2025 年 12 月 15 日 16：34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserAttributeCostAllocationPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/user-attribute-cost-
allocation-data.amazonaws.com/AWSServiceRoleForUserAttributeCostAllocation"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSUserNotificationsServiceLinkedRolePolicy

描述：允許 AWS 使用者通知代表您呼叫 AWS 服務。

AWSUserNotificationsServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- **建立時間**：2023 年 4 月 19 日 13：28 UTC
- **編輯時間**：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    {
      "Sid" : "AllowOrgsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "notifications.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationNotificationConfigurationDistribution",
      "Effect" : "Allow",
      "Action" : [
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteNotificationConfiguration",
        "notifications:CreateEventRule",
        "notifications:UpdateEventRule",
        "notifications:DeleteEventRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSVendorInsightsAssessorFullAccess

描述：提供檢視合格 Vendor Insights 資源和管理 Vendor Insights 訂閱的完整存取權

AWSVendorInsightsAssessorFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSVendorInsightsAssessorFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 7 月 26 日 15：05 UTC
- 編輯時間：2022 年 12 月 1 日 00：51 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSVendorInsightsAssessorReadOnly

描述：提供唯讀存取權，以檢視具備權限的 Vendor Insights 資源

AWSVendorInsightsAssessorReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSVendorInsightsAssessorReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 7 月 26 日 15：05 UTC
- 編輯時間：2022 年 12 月 1 日 00：55 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSVendorInsightsVendorFullAccess

描述：提供建立和管理 Vendor Insights 資源的完整存取權

`AWSVendorInsightsVendorFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSVendorInsightsVendorFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 7 月 26 日 15：05 UTC

- **編輯時間**：2023 年 10 月 19 日 01：41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSVendorInsightsVendorReadOnly

描述：提供唯讀存取權以檢視 Vendor Insights 資源

AWSVendorInsightsVendorReadOnly 是 AWS 受管政策。

使用此政策

您可以將 AWSVendorInsightsVendorReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 7 月 26 日 15：05 UTC
- 編輯時間：2022 年 12 月 1 日 00：54 UTC
- ARN: arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSVpcLatticeServiceRolePolicy

描述：允許 VPC Lattice 代表您存取 AWS 資源。

`AWSVpcLatticeServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 30 日 20：47 UTC
- 編輯時間：2024 年 12 月 1 日 14：06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    },
    {
      "Sid" : "VpcLatticeDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithSubnetAndSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VpcLatticeTagNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
```

```
      "Sid" : "VpcLatticeMutateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceActionsIpAddressActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeAssociateHostedZoneToVpc",
      "Effect" : "Allow",
      "Action" : [
        "route53:AssociateVPCWithHostedZone"
      ],
```

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSVPCS2SVpnServiceRolePolicy

描述：允許Site-to-Site建立和管理與 VPN 連線相關的資源。

AWSVPCS2SVpnServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 8 月 6 日 14：13 UTC
- 編輯時間：2025 年 5 月 15 日 16：52 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpnConnectionSecretsManagement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "s2svpn",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpnConnectionSecretsCreation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "s2svpn!*"
        }
```

```
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSVPCTransitGatewayServiceRolePolicy

描述：允許 VPC Transit Gateway 建立和管理 Transit Gateway VPC Attachments 的必要資源。

`AWSVPCTransitGatewayServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 26 日 16：21 UTC
- 編輯時間：2021 年 4 月 15 日 16：31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSVPCVerifiedAccessServiceRolePolicy

描述：啟用 AWS Verified Access 服務以代表您佈建端點的政策

AWSVPCVerifiedAccessServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 29 日 03：35 UTC
- 編輯時間：2023 年 11 月 17 日 21：03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

AWSWAFConsoleFullAccess

描述：透過 提供 AWS WAF 的完整存取權 AWS 管理主控台。請注意，此政策也授予列出和更新 Amazon CloudFront 分佈的許可、檢視彈性負載平衡器 on AWS Elastic Load Balancing 的許可、檢視 Amazon API Gateway REST APIs許可、列出和檢視 Amazon CloudWatch 指標的許可，以及檢視帳戶內啟用區域的許可。

AWSWAFConsoleFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSWAFConsoleFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 4 月 6 日 18：38 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess

政策版本

政策版本： v20 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
```

```
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant",
        "cloudfront:AssociateDistributionTenantWebACL",
        "cloudfront:DisassociateDistributionTenantWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
```

```
        "appsync:ListApis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "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"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : "pricingplanmanager:ListSubscriptions",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSWAFConsoleReadOnlyAccess

描述：透過 提供 AWS WAF 的唯讀存取權 AWS 管理主控台。請注意，此政策也授予列出 Amazon CloudFront 分佈的許可、檢視 AWS Elastic Load Balancing 上負載平衡器的許可、檢視 Amazon API Gateway REST APIs許可、列出和檢視 Amazon CloudWatch 指標的許可，以及檢視帳戶內啟用區域的許可。

`AWSWAFConsoleReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSWAFConsoleReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 4 月 6 日 18：43 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

政策版本

政策版本： v19 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
```

```
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
```

```
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListSubscriptionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSWAFFullAccess

描述：提供 AWS WAF 動作的完整存取權。

AWSWAFFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSWAFFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 10 月 6 日 20：44 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFFullAccess

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
```

```
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
```

```
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
```

```
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSWAFReadOnlyAccess

描述：提供 AWS WAF 動作的唯讀存取權。

AWSWAFReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSWAFReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 10 月 6 日 20：43 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
```

```
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
```

```
      ]
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
```

```
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSWellArchitectedDiscoveryServiceRolePolicy

描述：允許 WellArchitected 代表客戶存取與 WellArchitected 資源相關的 AWS 服務和資源。

`AWSWellArchitectedDiscoveryServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 4 月 26 日 18：36 UTC
- 編輯時間：2023 年 4 月 26 日 18：36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSWellArchitectedOrganizationsServiceRolePolicy

描述：允許 Well-Architected 代表您存取 Organizations。

`AWSWellArchitectedOrganizationsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 6 月 23 日 17：15 UTC
- 編輯時間：2022 年 7 月 25 日 18：03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSWickrFullAccess

描述：此政策會授予 Wickr 服務的完整管理許可，包括 下的 Wickr 管理函數 AWS 管理主控台。

AWSWickrFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSWickrFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 11 月 27 日 20：36 UTC
- 編輯時間：2022 年 11 月 27 日 20：36 UTC
- ARN: arn:aws:iam::aws:policy/AWSWickrFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSXrayCrossAccountSharingConfiguration

描述：提供管理可觀測性 Access Manager 連結和建立 X-Ray 追蹤共用的功能

`AWSXrayCrossAccountSharingConfiguration` 是 AWS 受管政策。

使用此政策

您可以將 `AWSXrayCrossAccountSharingConfiguration` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 27 日 13：46 UTC

- **編輯時間**：2022 年 11 月 27 日 13：46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSXRayDaemonWriteAccess

描述：允許 AWS X-Ray 協助程式將原始追蹤區段資料轉送至服務的 API，並擷取 X-Ray SDK 要使用的取樣資料（規則、目標等）。

`AWSXRayDaemonWriteAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSXRayDaemonWriteAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 8 月 28 日，UTC 23：00
- 編輯時間：2024 年 2 月 13 日 21：58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

政策版本

政策版本： v2（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

AWSXrayFullAccess

Description： AWS X-Ray 完整存取受管政策

AWSXrayFullAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSXrayFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 12 月 1 日 18：30 UTC
- 編輯時間：2024 年 4 月 11 日 17：07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSXrayReadOnlyAccess

Description： AWS X-Ray 唯讀受管政策

AWSXrayReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 AWSXrayReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 12 月 1 日 18：27 UTC
- 編輯時間：2024 年 2 月 14 日 00：35 UTC
- ARN: arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSXrayWriteOnlyAccess

Description： AWS X-Ray 僅寫入受管政策

`AWSXrayWriteOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `AWSXrayWriteOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2016 年 12 月 1 日 18：19 UTC
- **編輯時間**：2018 年 8 月 28 日，UTC 23：03
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSZonalAutoshiftPracticeRunSLRPolicy

描述：提供 ARC 區域轉移實務執行的管理存取權，以及 CloudWatch 警示狀態的存取權，以監控實務執行。

AWSZonalAutoshiftPracticeRunSLRPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 29 日 17：34 UTC
- 編輯時間：2025 年 6 月 30 日 17：07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AutoshiftPracticeCheckPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

AWSZoneGroupAccessManagementServiceRolePolicy

描述：提供對支援組織區域群組存取管理所需的 APIs 的唯讀存取權。

AWSZoneGroupAccessManagementServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 7 月 1 日 19：07 UTC
- 編輯時間：2025 年 7 月 1 日 19：07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZoneGroupAccessManagementServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

BatchServiceRolePolicy

描述：提供 AWS Batch 服務管理所需資源的存取權，包括 Amazon EC2 和 Amazon ECS 資源。

`BatchServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 3 月 10 日 06：55 UTC
- 編輯時間：2023 年 12 月 5 日 22：52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

BedrockAgentCoreFullAccess

描述：提供 Bedrock AgentCore 的完整存取權，以及對相關服務的有限存取權

BedrockAgentCoreFullAccess 是 AWS 受管政策。

使用此政策

您可以將 BedrockAgentCoreFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 7 月 16 日 13：37 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/BedrockAgentCoreFullAccess

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAgentCoreFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:*"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:*"
    },
    {
      "Sid" : "IAMListAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "BedrockAgentCorePassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*BedrockAgentCore*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:bedrock-agentcore*"
    },
    {
      "Sid" : "BedrockAgentCoreKMSReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:ListGrants"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "bedrock-agentcore.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSGrantsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "bedrock-agentcore.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:bedrock-agentcore-gateway:arn" : "arn:aws:bedrock-
agentcore:*:*:gateway/*"
```

```
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-gateway-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-agentcore.amazonaws.com",
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreGatewayLambdaAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:*"
      ]
    },
    {
      "Sid" : "BedrockAgentCoreGatewayApiGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*/stages/*/exports/*"
      ]
```

```
    },
    {
      "Sid" : "LoggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "ObservabilityReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "oam:ListSinks",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
```

```
        "xray:CancelTraceRetrieval",
        "logs:DescribeLogGroups",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchXRayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSegmentDestination",
        "xray:UpdateTraceSegmentDestination",
        "xray:GetIndexingRules",
        "xray:UpdateIndexingRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "TransactionSearchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "TransactionSearchApplicationSignalsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:StartDiscovery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CreateBedrockAgentCoreNetworkServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/network.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreNetwork",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreRuntimeIdentityServiceLinkedRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/runtime-identity.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreRuntimeIdentity",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "runtime-identity.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3WriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-runtime-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
```

```
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeECRAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:DescribeImages",
        "ecr:ListImages"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/evaluations/*"
      ]
    },
```

```
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogIndexAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutIndexPolicy",
        "logs:DescribeIndexPolicies"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/spans",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockInvokeAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

BedrockAgentCoreNetworkServiceRolePolicy

描述：允許存取在 VPC 模式下執行 Amazon Bedrock AgentCore 所需的其他 AWS 服務資源

BedrockAgentCoreNetworkServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 9 月 19 日，UTC 22：04
- 編輯時間：2025 年 9 月 19 日，UTC 22：04
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreNetworkServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateEniInAnySubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Sid" : "AllowCreateEniWithSecurityGroups",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "AllowCreateEniWithBedrockManagedRequestTag",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonBedrockAgentCoreManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowTagEniOnCreate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowManageEniWhenBedrockManaged",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGetSecurityGroupsForVpc",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:GetSecurityGroupsForVPC"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowDescribeNetworkingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

BedrockAgentCoreRuntimeIdentityServiceRolePolicy

描述：允許存取 Amazon Bedrock AgentCore 執行期身分驗證和授權所需的身分和字符管理資源。

`BedrockAgentCoreRuntimeIdentityServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 10 月 11 日 01：04 UTC
- 編輯時間：2025 年 10 月 11 日 01：04 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Sid" : "AllowWorkloadIdentityAccess",
    "Effect" : "Allow",
    "Action" : [
      "bedrock-agentcore:GetWorkloadAccessToken",
      "bedrock-agentcore:GetWorkloadAccessTokenForJWT",
      "bedrock-agentcore:GetWorkloadAccessTokenForUserId"
    ],
    "Resource" : [
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default",
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default/workload-identity/*"
    ]
  }
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

Billing

描述：授予帳單和成本管理的許可。這包括檢視帳戶用量，以及檢視和修改預算和付款方式。

`Billing` 是 AWS 受管政策。

使用此政策

您可以將 Billing 連接至使用者、群組與角色。

政策詳細資訊

- 類型：任務函數政策
- 建立時間：2016 年 11 月 10 日 17：33 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/job-function/Billing

政策版本

政策版本： v27 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:CreateBillingView",
        "billing:DeleteBillingView",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetContractInformation",
        "billing:GetCredits",
```

```
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:GetResourcePolicy",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billing:TagResource",
        "billing:UntagResource",
        "billing:UpdateBillingPreferences",
        "billing:UpdateBillingView",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
        "budgets:UpdateBudgetAction",
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce:DeleteCostCategoryDefinition",
        "ce:DeleteNotificationSubscription",
        "ce:DeleteReport",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:TagResource",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:UpdateNotificationSubscription",
        "ce:UpdatePreferences",
        "ce:UpdateReport",
        "ce:UpdateCostCategoryDefinition",
        "ce:UntagResource",
        "ce:StartCostAllocationTagBackfill",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
```

```
        "ce:GetDimensionValues",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:ModifyReportDefinition",
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:CreateInvoiceUnit",
        "invoicing:DeleteInvoiceUnit",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:CreateProcurementPortalPreference",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:PutProcurementPortalPreference",
        "invoicing:UpdateProcurementPortalPreferenceStatus",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:DeleteProcurementPortalPreference",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "invoicing:StartInvoiceCorrection",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "invoicing:TagResource",
        "invoicing:UntagResource",
        "invoicing:UpdateInvoiceUnit",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:CreateFinancingApplication",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetFinancingApplication",
```

```
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "payments:ListPaymentInstruments",
        "payments:MakePayment",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:UpdateFinancingApplication",
        "payments:UpdatePaymentInstrument",
        "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

BudgetsServiceRolePolicy

描述：允許 Budgets 驗證對跨帳戶界限共用的帳單檢視的存取權。

BudgetsServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 7 月 30 日 21：07 UTC
- 編輯時間：2025 年 7 月 30 日 21：07 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/BudgetsServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CertificateManagerServiceRolePolicy

描述：Amazon Certificate Manager Service 角色政策

`CertificateManagerServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 6 月 25 日 17：56 UTC
- 編輯時間：2020 年 6 月 25 日 17：56 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ClientVPNServiceConnectionsRolePolicy

描述：啟用 AWS Client VPN 以管理 Client VPN 端點連線的政策。

`ClientVPNServiceConnectionsRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 8 月 12 日 19：48 UTC
- 編輯時間：2020 年 8 月 12 日 19：48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ClientVPNServiceRolePolicy

描述：啟用 AWS Client VPN 以管理 Client VPN 端點的政策。

ClientVPNServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 12 月 10 日 21：20 UTC
- 編輯時間：2020 年 8 月 12 日，UTC 19：39
- ARN: arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudFormationStackSetsOrgAdminServiceRolePolicy

描述：CloudFormation StackSets 的服務角色（組織主帳戶）

`CloudFormationStackSetsOrgAdminServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 12 月 10 日 00：20 UTC
- 編輯時間：2019 年 12 月 10 日 00：20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudFormationStackSetsOrgMemberServiceRolePolicy

描述：CloudFormation StackSets 的服務角色 （組織成員帳戶）

`CloudFormationStackSetsOrgMemberServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 12 月 9 日 23：52 UTC
- 編輯時間：2019 年 12 月 9 日 23：52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

CloudFrontFullAccess

描述：提供 CloudFront 主控台的完整存取權，以及透過 列出 Amazon S3 儲存貯體的功能 AWS 管理主控台。

`CloudFrontFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudFrontFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

政策版本

政策版本： v14 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "wafv2:CreateWebACL",
        "kinesis:ListStreams",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:CreateSubscription"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "cfrequestcertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudfront.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cffdescribestream",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:*"
    },
    {
      "Sid" : "ppmFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:AssociateResourcesToSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange",
        "pricingplanmanager:DisassociateResourcesFromSubscription",
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    }
```

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudFrontReadOnlyAccess

描述：提供 CloudFront 分佈組態資訊的存取權，並透過 列出分佈 AWS 管理主控台。

`CloudFrontReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudFrontReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "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",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudHSMServiceRolePolicy

描述：允許存取 CloudHSM 使用或管理 AWS 的資源

CloudHSMServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 11 月 6 日 19：12 UTC
- 編輯時間：2017 年 11 月 6 日 19：12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudSearchFullAccess

描述：提供 Amazon CloudSearch 組態服務的完整存取權。

`CloudSearchFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudSearchFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2015 年 2 月 6 日 18：39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudSearchReadOnlyAccess

描述：提供 Amazon CloudSearch 組態服務的唯讀存取權。

`CloudSearchReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudSearchReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2015 年 2 月 6 日 18：39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

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

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudTrailEventContext

描述：此服務連結角色可讓 CloudTrail 取得資源標籤，並將其新增至資源擁有者的 CloudTrail 事件。

`CloudTrailEventContext` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 5 月 15 日 13：52 UTC
- 編輯時間：2025 年 5 月 15 日 13：52 UTC

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

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventContextPermissionForTag",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleCreation",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.tag"
        },
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:detail-type" : "Tag Change on Resource",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowEventBridgeRuleWrite",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleRead",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*"
    },
    {
      "Sid" : "AllowEventBridgeRuleList",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

CloudTrailServiceRolePolicy

描述：CloudTrail ServiceLinkedRole 的許可政策

`CloudTrailServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 10 月 24 日，UTC 21：21
- 編輯時間：2023 年 11 月 27 日 01：18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatch-CrossAccountAccess

描述：允許 CloudWatch 代表目前帳戶在遠端帳戶中擔任 CloudWatch-CrossAccountSharing 角色，以顯示跨帳戶、跨區域的資料

`CloudWatch-CrossAccountAccess` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 7 月 23 日 09：59 UTC
- 編輯時間：2019 年 7 月 23 日 09：59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchActionsEC2Access

描述：提供 CloudWatch 警示和指標以及 EC2 中繼資料的唯讀存取權。提供停止、終止和重新啟動 EC2 執行個體的存取權。

`CloudWatchActionsEC2Access` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchActionsEC2Access` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 7 月 7 日 00：00 UTC
- 編輯時間：2015 年 7 月 7 日 00：00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchAgentAdminPolicy

描述：使用 AmazonCloudWatchAgent 所需的完整許可。

CloudWatchAgentAdminPolicy 是 AWS 受管政策。

使用此政策

您可以將 CloudWatchAgentAdminPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 3 月 7 日 00：52 UTC
- 編輯時間：2024 年 2 月 5 日 20：59 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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-*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudWatchAgentServerPolicy

描述：在伺服器上使用 AmazonCloudWatchAgent 所需的許可

`CloudWatchAgentServerPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchAgentServerPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 3 月 7 日 01：06 UTC
- 編輯時間：2024 年 2 月 6 日 16：37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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-*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudWatchApplicationInsightsFullAccess

描述：提供 CloudWatch Application Insights 和必要相依性的完整存取權。

`CloudWatchApplicationInsightsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchApplicationInsightsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 11 月 24 日 18：44 UTC
- 編輯時間：2022 年 1 月 25 日 17：51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudWatchApplicationInsightsReadOnlyAccess

描述：提供 CloudWatch Application Insights 的唯讀存取權。

`CloudWatchApplicationInsightsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchApplicationInsightsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 11 月 24 日 18：48 UTC

- **編輯時間**：2020 年 11 月 24 日 18：48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudwatchApplicationInsightsServiceLinkedRolePolicy

描述：Cloudwatch Application Insights 服務連結角色政策

`CloudwatchApplicationInsightsServiceLinkedRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 12 月 1 日 16：22 UTC
- 編輯時間：2024 年 7 月 25 日 16：24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

政策版本

政策版本： v25 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:CreateStack",
        "cloudFormation:UpdateStack",
        "cloudFormation:DeleteStack",
        "cloudFormation:DescribeStackResources",
        "cloudFormation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "CloudFormationStacks",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudFormation:DescribeStacks",
        "cloudFormation:ListStackResources",
        "cloudFormation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ResourceGroups",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationInsightsResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "ElasticLoadBalancing",
      "Effect" : "Allow",
```

```
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
    },
    {
      "Sid" : "SSMAssociation",
      "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"
      ]
    },
    {
      "Sid" : "SSMOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:CreateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:UpdateOpsItem",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMTags",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "SSMGetCommandInvocation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommand",
      "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"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Lambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "EventBridgeManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "XRay",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetTraceGraph"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscaling",
      "Effect" : "Allow",
      "Action" : [
```

```
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "States",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "APIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECSCluster",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateClusterSettings"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "EKS",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:GetSMSAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsDeleteSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsCreateSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
      ]
    },
    {
```

```
      "Sid" : "EFS",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53Resolver",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchApplicationSignalsFullAccess

描述：提供 CloudWatch Application Signals 服務的完整存取權，以及使用和操作此服務所需的相依性範圍存取權。

`CloudWatchApplicationSignalsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchApplicationSignalsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 6 月 6 日 22：50 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "application-signals:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchCreateRumMetricDefinitions",
```

```
        "rum:BatchDeleteRumMetricDefinitions",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:PutRumMetricsDestination",
        "rum:UpdateRumMetricDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
```

```
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:cloudwatch-application-signals-*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
      "Effect" : "Allow",
      "Action" : "sns:ListTopics",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
```

```
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
```

```
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchApplicationSignalsReadOnlyAccess

描述：提供 CloudWatch Application Signals 服務的唯讀存取權，以及使用此服務所需的相依性範圍存取權

`CloudWatchApplicationSignalsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchApplicationSignalsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 6 月 6 日 22：48 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "application-signals:ListServiceStates",
        "application-signals:ListAuditFindings",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListEntityEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
```

```
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudWatchApplicationSignalsServiceRolePolicy

描述：政策授予 CloudWatch Application Signals 許可，以從其他相關 AWS 服務收集監控和標記資料。

`CloudWatchApplicationSignalsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 9 日 18：09 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "xray:GetServiceGraph"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWListMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "CWGetMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ApplicationSignalsPermission",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:GetServiceLevelObjective"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2AutoScalingPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudTrailServiceLinkedChannelCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-signals/*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

CloudWatchAutomaticDashboardsAccess

描述：提供用於顯示 CloudWatch Automatic Dashboards 的非 CloudWatch APIs 的存取權，包括 Lambda 函數等物件的內容

`CloudWatchAutomaticDashboardsAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchAutomaticDashboardsAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 7 月 23 日 10：01 UTC
- 編輯時間：2021 年 4 月 20 日 13：05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchCrossAccountSharingConfiguration

描述：提供管理可觀測性 Access Manager 連結和建立 CloudWatch 資源共用的功能

`CloudWatchCrossAccountSharingConfiguration` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchCrossAccountSharingConfiguration` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 11 月 27 日 14：01 UTC
- 編輯時間：2022 年 11 月 27 日 14：01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchEventsBuiltInTargetExecutionAccess

描述：允許 Amazon CloudWatch Events 中的內建目標代表您執行 EC2 動作。

CloudWatchEventsBuiltInTargetExecutionAccess 是 AWS 受管政策。

使用此政策

您可以將 CloudWatchEventsBuiltInTargetExecutionAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 1 月 14 日 18：35 UTC
- 編輯時間：2016 年 1 月 14 日 18：35 UTC
- ARN: arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchEventsFullAccess

描述：提供 Amazon CloudWatch Events 的完整存取權。

`CloudWatchEventsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchEventsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2016 年 1 月 14 日 18：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchEventsInvocationAccess

描述：允許 Amazon CloudWatch Events 將事件轉送至您帳戶中 AWS Kinesis Streams 中的串流。

`CloudWatchEventsInvocationAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchEventsInvocationAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2016 年 1 月 14 日 18：36 UTC
- 編輯時間：2016 年 1 月 14 日 18：36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchEventsReadOnlyAccess

描述：提供 Amazon CloudWatch Events 的唯讀存取權。

`CloudWatchEventsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchEventsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 1 月 14 日 18：27 UTC
- 編輯時間：2022 年 12 月 1 日 16：29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchEventsServiceRolePolicy

描述：允許 AWS CloudWatch 透過警示和事件代表您執行動作。

`CloudWatchEventsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 11 月 17 日 00：42 UTC
- 編輯時間：2017 年 11 月 17 日 00：42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchFullAccess

描述：提供 CloudWatch 的完整存取權。

`CloudWatchFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2022 年 11 月 27 日 13：23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchFullAccessV2

描述：提供 CloudWatch 的完整存取權。

`CloudWatchFullAccessV2` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchFullAccessV2` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 8 月 1 日 11：32 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:*",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:CreateCentralizationRuleForOrganization",
        "observabilityadmin:UpdateCentralizationRuleForOrganization",
        "observabilityadmin:DeleteCentralizationRuleForOrganization",
        "observabilityadmin:StartTelemetryEvaluation",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:StopTelemetryEvaluation",
        "observabilityadmin:StartTelemetryEvaluationForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:ListResourceTelemetryForOrganization",
```

```
        "observabilityadmin:StopTelemetryEvaluationForOrganization",
        "observabilityadmin:CreateTelemetryRule",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:UpdateTelemetryRule",
        "observabilityadmin:DeleteTelemetryRule",
        "observabilityadmin:CreateTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:UpdateTelemetryRuleForOrganization",
        "observabilityadmin:DeleteTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:StartTelemetryEnrichment",
        "observabilityadmin:StopTelemetryEnrichment",
        "observabilityadmin:TagResource",
        "observabilityadmin:UntagResource",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:CreateTelemetryPipeline",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:UpdateTelemetryPipeline",
        "observabilityadmin:DeleteTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:CreateS3TableIntegration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:DeleteS3TableIntegration",
        "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/*"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "CloudWatchResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "logs.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" :
 "arn:aws:observabilityadmin:*:*:s3tableintegration/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "logs.amazonaws.com",
            "telemetry-pipelines.observabilityadmin.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:observabilityadmin:*:*:telemetry-
pipeline/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketEncryption"
```

```
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "observabilityadmin.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:PutTableBucketPolicy"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudWatchInternetMonitorFullAccess

描述：提供使用 Amazon CloudWatch 網路監視器之動作的完整存取權。也提供對其他服務的存取權，例如 Amazon CloudWatch、Amazon EC2、Amazon CloudFront、Amazon WorkSpaces 和 Elastic Load Balancing，這些服務是使用網路監視器服務來監控和儲存應用程式流量的相關資訊所必需。

`CloudWatchInternetMonitorFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchInternetMonitorFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2024 年 10 月 22 日 21：02 UTC
- **編輯時間**：2024 年 10 月 22 日 21：02 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessActions",
      "Effect" : "Allow",
      "Action" : [
        "internetmonitor:CreateMonitor",
        "internetmonitor:DeleteMonitor",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:Link",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "internetmonitor:TagResource",
        "internetmonitor:UntagResource",
        "internetmonitor:UpdateMonitor"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ServiceLinkedRoleActions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "internetmonitor.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RolePolicyActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/aws-service-role/
CloudWatchInternetMonitorServiceRolePolicy"
        }
      }
    },
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchInternetMonitorReadOnlyAccess

描述：提供使用 Amazon CloudWatch 網路監視器之動作的唯讀存取權。也提供 Amazon CloudWatch 中其他服務的存取權，包括擷取 CloudWatch 指標相關資訊和管理日誌查詢的政策，這些查詢是使用網路監視器服務監控和儲存應用程式流量相關資訊所必需。

`CloudWatchInternetMonitorReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchInternetMonitorReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 12 日 23：11 UTC
- 編輯時間：2024 年 11 月 12 日 23：11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudWatchInternetMonitorServiceRolePolicy

描述：允許網路監視器代表您存取 EC2、Workspaces 和 CloudFront 資源，以及其他必要的服務。

`CloudWatchInternetMonitorServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 27 日 17：46 UTC
- 編輯時間：2023 年 7 月 20 日 04：46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

CloudWatchLambdaApplicationSignalsExecutionRolePolicy

描述：提供 X-Ray 和 CloudWatch Application Signals 日誌群組的寫入存取權。

`CloudWatchLambdaApplicationSignalsExecutionRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 CloudWatchLambdaApplicationSignalsExecutionRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 10 月 16 日 19：09 UTC
- 編輯時間：2024 年 10 月 16 日 19：09 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLambdaApplicationSignalsExecutionRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsXrayWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchLambdaInsightsExecutionRolePolicy

描述：Lambda Insights 延伸模組所需的政策

`CloudWatchLambdaInsightsExecutionRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchLambdaInsightsExecutionRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2020 年 10 月 7 日 19：27 UTC
- **編輯時間**：2020 年 10 月 7 日 19：27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchLogsAPIKeyAccess

描述：授予使用 API 金鑰身分驗證呼叫 CloudWatch Logs 的許可。

`CloudWatchLogsAPIKeyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchLogsAPIKeyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2026 年 2 月 20 日 19：42 UTC
- 編輯時間：2026 年 2 月 20 日 19：42 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsAPIKeyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogsAPIs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CallWithBearerToken",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAPIs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "logs.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSDescribeAPIs",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "logs.*.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchLogsCrossAccountSharingConfiguration

描述：提供管理可觀測性 Access Manager 連結和建立 CloudWatch Logs 資源共用的功能

CloudWatchLogsCrossAccountSharingConfiguration 是 AWS 受管政策。

使用此政策

您可以將 CloudWatchLogsCrossAccountSharingConfiguration 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 27 日 13：55 UTC
- 編輯時間：2022 年 11 月 27 日 13：55 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchLogsFullAccess

描述：提供 CloudWatch Logs 的完整存取權

`CloudWatchLogsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchLogsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- **建立時間**：2015 年 2 月 6 日 18：40 UTC
- **編輯時間**：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchLogsReadOnlyAccess

描述：提供 CloudWatch Logs 的唯讀存取權

`CloudWatchLogsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchLogsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchNetworkFlowMonitorAgentPublishPolicy

描述：您可以在連接到 Amazon EC2 和 Amazon EKS 執行個體資源的 IAM 角色中使用此政策，以將遙測報告（指標）傳送至網路流量監控端點。

`CloudWatchNetworkFlowMonitorAgentPublishPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchNetworkFlowMonitorAgentPublishPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2024 年 12 月 1 日 22：51 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC

- ARN: `arn:aws:iam::aws:policy/CloudWatchNetworkFlowMonitorAgentPublishPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkflowmonitor:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchNetworkFlowMonitorServiceRolePolicy

描述：您無法將 CloudWatchNetworkFlowMonitorServiceRolePolicy 連接至 IAM 實體。此政策會連結至名為 AWSServiceRoleForNetworkFlowMonitor 的服務連結角色，該角色會將 Network Flow Monitor 代理程式收集的網路遙測彙總結果發布至 CloudWatch。它還允許服務使用 AWS Organizations 來取得多帳戶案例的資訊。

CloudWatchNetworkFlowMonitorServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 12 月 1 日 22：36 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorServiceRolePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkFlowMonitor"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

描述：您無法將 CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy 連接至 IAM 實體。此政策會連接到名為 AWSServiceRoleForNetworkFlowMonitor_Topology 的服務連結角色，這會產生您帳戶中 Network Flow Monitor 所使用的資源拓撲快照。

`CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- **建立時間**：2024 年 12 月 1 日 22：51 UTC
- **編輯時間**：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeCustomerGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "VPCEndpointStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchNetworkMonitorServiceRolePolicy

描述：允許 CloudWatch Network Monitor 存取和管理 EC2 和 VPC 資源、將資料發佈至 CloudWatch，以及代表您存取其他必要的服務。

`CloudWatchNetworkMonitorServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 12 月 21 日 18：53 UTC
- 編輯時間：2025 年 12 月 12 日 22：04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchOpenSearchDashboardAccess

描述：此政策提供使用者在 CloudWatch Logs 主控台上檢視 OpenSearch 儀表板的存取權。

`CloudWatchOpenSearchDashboardAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchOpenSearchDashboardAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 1 日 21：06 UTC

- **編輯時間**：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDirectQueryStatusAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudWatchOpenSearchDashboardsFullAccess

描述：此政策提供使用者建立與 OpenSearch 整合的存取權，以在 CloudWatch Logs 主控台上建立、更新、刪除或檢視儀表板。

CloudWatchOpenSearchDashboardsFullAccess 是 AWS 受管政策。

使用此政策

您可以將 CloudWatchOpenSearchDashboardsFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 1 日 21：06 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardsFullAccess

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DeleteIntegration",
        "logs:PutIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsOpensearchCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsObservabilityCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "CloudWatchLogsCollectionRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:CreateApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:DeleteCollection"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:UpdateApplication",
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateSecurityPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsIndexPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:CreateLifecyclePolicy",
        "aoss:DeleteLifecyclePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:index" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSRequestQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
```

```
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsStartDirectQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:StartDirectQuery",
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource",
        "es:DeleteDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "directquery.opensearchservice.amazonaws.com",
```

```
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAossTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:TagResource"
      ],
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsApplicationTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:application/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsDataSourceTagsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CloudWatchReadOnlyAccess

描述：提供 CloudWatch 的唯讀存取權。

`CloudWatchReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2015 年 2 月 6 日 18：40 UTC
- **編輯時間**：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

政策版本

政策版本： v24 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudtrail:ListChannels",
        "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",
```

```
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchReadOnlyGetRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
```

```
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchSyntheticsFullAccess

描述：提供 CloudWatch Synthetics 的完整存取權。

`CloudWatchSyntheticsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchSyntheticsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 11 月 25 日 17：39 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

政策版本

政策版本： v13 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
        "logs:GetLogRecord",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:GetLogGroupFields"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/cwsyn-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource"
      ],
      "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:*",
        "arn:aws:lambda:*:*:layer:Synthetics_Selenium:*",
        "arn:aws:lambda:*:*:layer:AWS-CW-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"
          ]
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CloudWatchSyntheticsReadOnlyAccess

描述：提供 CloudWatch Synthetics 的唯讀存取權。

`CloudWatchSyntheticsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CloudWatchSyntheticsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 11 月 25 日 17：45 UTC
- 編輯時間：2020 年 3 月 6 日 19：26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ComprehendDataAccessRolePolicy

描述： AWS Comprehend 服務角色的政策，允許存取 S3 資源以進行資料存取

`ComprehendDataAccessRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ComprehendDataAccessRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2019 年 3 月 6 日 22：28 UTC
- 編輯時間：2019 年 3 月 6 日 22：28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

政策版本

政策版本： v1 （ 預設 ）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ComprehendFullAccess

描述：提供 Amazon Comprehend 的完整存取權。

ComprehendFullAccess 是 AWS 受管政策。

使用此政策

您可以將 ComprehendFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 29 日 18：08 UTC
- 編輯時間：2017 年 12 月 5 日 01：36 UTC
- ARN: arn:aws:iam::aws:policy/ComprehendFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ComprehendMedicalFullAccess

描述：提供 Amazon Comprehend Medical 的完整存取權

`ComprehendMedicalFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ComprehendMedicalFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 11 月 27 日 17：55 UTC
- 編輯時間：2018 年 11 月 27 日 17：55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ComprehendReadOnly

描述：提供 Amazon Comprehend 的唯讀存取權。

`ComprehendReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `ComprehendReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2017 年 11 月 29 日 18：10 UTC
- 編輯時間：2022 年 4 月 26 日，UTC 21：32
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ComputeOptimizerAutomationServiceRolePolicy

描述：ComputeOptimizerAutomationServiceRolePolicy 受管政策會連接到允許 Compute Optimizer 代表您執行動作的服務連結角色

`ComputeOptimizerAutomationServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 11 月 15 日 01：19 UTC
- 編輯時間：2025 年 11 月 15 日 01：19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerAutomationServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSVolumeModification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/exclude-from-compute-optimizer-automation" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "RollbackEBSVolumeDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ComputeOptimizerReadOnlyAccess

描述：提供 ComputeOptimizer 的唯讀存取權。

`ComputeOptimizerReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ComputeOptimizerReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 3 月 7 日 00：11 UTC
- 編輯時間：2024 年 11 月 20 日 21：08 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "computeOptimizerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
```

```
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetIdleRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ComputeOptimizerServiceRolePolicy

描述：允許 ComputeOptimizer 代您呼叫 AWS 服務並收集工作負載詳細資訊。

ComputeOptimizerServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 12 月 3 日 08：45 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ConfigConformsServiceRolePolicy

描述：AWSConfig 建立一致性套件所需的政策

ConfigConformsServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 7 月 25 日 21：38 UTC
- 編輯時間：2023 年 1 月 12 日 04：17 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ConsoleFullAccessFromVercel

描述：與透過 Vercel Marketplace 整合建立的帳戶搭配使用 AWS。提供管理與 Vercel Marketplace 整合之服務所有資源的存取權。

`ConsoleFullAccessFromVercel` 是 AWS 受管政策。

使用此政策

您可以將 `ConsoleFullAccessFromVercel` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 12 月 11 日 16：49 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/ConsoleFullAccessFromVercel

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dsql:UpdateCluster",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:UpdateTimeToLive",
```

```
        "dynamodb:ConditionCheckItem",
        "dynamodb:UntagResource",
        "dynamodb:PutItem",
        "dynamodb:ListTables",
        "dynamodb:DeleteItem",
        "dynamodb:Scan",
        "dynamodb:ListTagsOfResource",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:DescribeLimits",
        "dynamodb:UpdateTable",
        "dynamodb:GetRecords"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds-db:connect",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rds:RebootDBInstance",
        "rds:DeleteDBInstance",
        "rds:StartDBInstance",
        "rds:ModifyDBInstance",
        "rds:ApplyPendingMaintenanceAction",
        "rds:StartDBCluster",
        "rds:DeleteDBCluster",
        "rds:RebootDBCluster",
        "rds:CreateDBClusterEndpoint",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:FailoverDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:ModifyDBClusterParameterGroup",
        "rds:CopyDBClusterParameterGroup",
```

```
        "rds:ResetDBClusterParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:ModifyDBParameterGroup",
        "rds:CopyDBParameterGroup",
        "rds:DeleteDBParameterGroup",
        "rds:CreateDBParameterGroup",
        "rds:DeleteDBClusterAutomatedBackup",
        "rds:CopyDBClusterSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:CreateDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AuroraRestricted",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "aurora-postgresql"
        }
      }
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
```

```
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ConsoleViewOnlyAccessFromVercel

描述：與透過 Vercel Marketplace 整合建立的帳戶搭配使用 AWS。提供檢視與 Vercel Marketplace 整合之服務所有資源的存取權。

`ConsoleViewOnlyAccessFromVercel` 是 AWS 受管政策。

使用此政策

您可以將 `ConsoleViewOnlyAccessFromVercel` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 12 月 11 日 16：49 UTC
- 編輯時間：2026 年 2 月 18 日 19：27 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleViewOnlyAccessFromVercel`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CostOptimizationHubAdminAccess

描述：此受管政策提供管理員存取 Cost Optimization Hub 的權限。

`CostOptimizationHubAdminAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CostOptimizationHubAdminAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 12 月 19 日 00：03 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CostOptimizationHubReadOnlyAccess

描述：此受管政策提供 Cost Optimization Hub 的唯讀存取權。

`CostOptimizationHubReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `CostOptimizationHubReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 12 月 13 日 18：04 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

CostOptimizationHubServiceRolePolicy

描述：允許 Cost Optimization Hub 擷取組織資訊，並收集最佳化相關資料和中繼資料。

`CostOptimizationHubServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 11 月 26 日 08：03 UTC
- 編輯時間：2025 年 7 月 17 日 18：07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:GetCostAndUsage",
```

```
        "ce:GetDimensionValues"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

CustomerProfilesServiceLinkedRolePolicy

描述：允許 Amazon Connect Customer Profiles 代表您存取 AWS 服務和資源。

`CustomerProfilesServiceLinkedRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 3 月 7 日 22：56 UTC
- 編輯時間：2026 年 3 月 5 日 21：12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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_*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:PutProfileOutboundRequestBatch"
      ],
      "Resource" : [
        "arn:aws:connect-campaigns:*:*:campaign/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:BatchGetProfile",
        "profile:GetRecommender",
        "profile:GetCalculatedAttributeForProfile",
```

```
        "profile:GetProfileRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

DatabaseAdministrator

描述：授予設定和設定 AWS 資料庫 AWS 服務所需的服務和動作的完整存取許可。

DatabaseAdministrator 是 AWS 受管政策。

使用此政策

您可以將 DatabaseAdministrator 連接至使用者、群組與角色。

政策詳細資訊

- 類型：任務函數政策
- 建立時間：2016 年 11 月 10 日 17：25 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DatabaseAdministrator

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "pi:CreatePerformanceAnalysisReport",
        "pi:DeletePerformanceAnalysisReport",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetPerformanceAnalysisReport",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pi:ListPerformanceAnalysisReports",
        "pi:ListTagsForResource",
        "pi:TagResource",
        "pi:UntagResource",
        "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"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

DataScientist

描述：授予 AWS 資料分析服務的許可。

DataScientist 是 AWS 受管政策。

使用此政策

您可以將 DataScientist 連接至使用者、群組與角色。

政策詳細資訊

- 類型：任務函數政策
- 建立時間：2016 年 11 月 10 日 17：28 UTC
- 編輯時間：2019 年 12 月 3 日 16：48 UTC
- ARN: arn:aws:iam::aws:policy/job-function/DataScientist

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
          ]
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

DAXServiceRolePolicy

描述：此政策允許 DAX 代表客戶建立和管理網路介面、安全群組、子網路和 Vpc

`DAXServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 3 月 5 日 17：51 UTC
- 編輯時間：2018 年 3 月 5 日 17：51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

DeclarativePoliciesEC2Report

描述：提供執行 EC2 宣告政策帳戶狀態報告所需的唯讀 APIs的存取權。

`DeclarativePoliciesEC2Report` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 11 月 30 日 13：21 UTC
- 編輯時間：2024 年 11 月 30 日 13：21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DeclarativePoliciesEC2Report`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeclarativePoliciesEC2Report",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetAllowedImagesSettings",
        "ec2:DescribeVpcBlockPublicAccessOptions"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

描述：支援 Amazon DynamoDB 的 Amazon CloudWatch Contributor Insights 所需的許可。DynamoDB

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 15 日 21：13 UTC
- 編輯時間：2019 年 11 月 15 日 21：13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

DynamoDBGlobalTableSettingsManagementServiceRolePolicy

描述：DynamoDB 管理全域資料表複本設定所需的許可

`DynamoDBGlobalTableSettingsManagementServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 10 月 15 日 17：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBGlobalTableSettingsManagementServiceRolePolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededToReplicateSettings",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*",
        "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/dynamodb/table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : [
            "dynamodb"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

DynamoDBKinesisReplicationServiceRolePolicy

描述：Provide AWS DynamoDB 存取 KinesisDataStreams

`DynamoDBKinesisReplicationServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 11 月 12 日 00：43 UTC
- 編輯時間：2020 年 11 月 12 日 00：43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

DynamoDBReplicationServiceRolePolicy

描述：DynamoDB 跨區域資料複寫所需的許可

DynamoDBReplicationServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 11 月 9 日，UTC 23：55
- 編輯時間：2024 年 1 月 8 日 20：10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

EC2FastLaunchFullAccess

描述：此政策授予 EC2 Fast Launch 動作的完整存取權

EC2FastLaunchFullAccess 是 AWS 受管政策。

使用此政策

您可以將 EC2FastLaunchFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 5 月 13 日 22：45 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/EC2FastLaunchFullAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2FastLaunch",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch",
        "ec2:DisableFastLaunch",
        "ec2:DescribeFastLaunchImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSnapshots",
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CreateVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ModifyDeleteVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:CreateSubnet",
        "ec2:ModifyVpcAttribute",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "EC2CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ManageSecurityGroupEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:RollbackStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/EC2FastLaunch*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchTemplateModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyLaunchTemplate",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "EC2LaunchInstanceWithVolAndInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "EC2Tags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "EC2ManageTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2fastlaunch.amazonaws.com/
AWSServiceRoleForEC2FastLaunch",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLRPassRole",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

EC2FastLaunchServiceRolePolicy

描述：政策授予 ec2fastlaunch，以準備和管理客戶帳戶中預先佈建的快照並發佈相關指標。

`EC2FastLaunchServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 1 月 10 日 13：08 UTC

- **編輯時間**：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRunInstances",
      "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/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "AllowRunInstancesOnFastLaunchCreatedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStopAndTerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateSnapshot",
      "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"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTags",
      "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"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDeleteSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDeleteVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
```

```
    {
      "Sid" : "AllowDeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeVolumes",
        "ec2:DescribeNetworkInterfaces",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EC2"
        }
      }
```

```
    },
    {
      "Sid" : "AllowEventsRuleMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2fastlaunch.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowEventsRuleNonMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeleteFastLaunchLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

EC2FleetTimeShiftableServiceRolePolicy

描述：將許可授予 EC2 機群以在未來啟動執行個體的政策。

EC2FleetTimeShiftableServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 12 月 23 日 19：47 UTC
- 編輯時間：2019 年 12 月 23 日 19：47 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

Ec2ImageBuilderCrossAccountDistributionAccess

描述：EC2 Image Builder 執行跨帳戶分佈所需的許可。

`Ec2ImageBuilderCrossAccountDistributionAccess` 是 AWS 受管政策。

使用此政策

您可以將 `Ec2ImageBuilderCrossAccountDistributionAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 9 月 30 日 19：22 UTC
- 編輯時間：2020 年 9 月 30 日 19：22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

政策版本

政策版本： v1 （ 預設 ）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

EC2ImageBuilderLifecycleExecutionPolicy

描述：EC2ImageBuilderLifecycleExecutionPolicy 政策授予 Image Builder 執行動作的許可，例如棄用或刪除 Image Builder 映像資源及其基礎資源 (AMIs、快照），以支援映像生命週期管理任務的自動化規則。

EC2ImageBuilderLifecycleExecutionPolicy 是 AWS 受管政策。

使用此政策

您可以將 EC2ImageBuilderLifecycleExecutionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 11 月 16 日 23：23 UTC
- 編輯時間：2023 年 11 月 16 日 23：23 UTC
- ARN: arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
```

```
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "DeprecatedBy"
        }
      }
    },
    {
      "Sid" : "ECRImagePermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ImageBuilderEC2TagServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "tag:GetResources",
        "imagebuilder:DeleteImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

EC2InstanceConnect

描述：允許客戶呼叫 EC2 Instance Connect，將暫時性金鑰發佈至其 EC2 執行個體，並透過 ssh 或 EC2 Instance Connect CLI 連線。

`EC2InstanceConnect` 是 AWS 受管政策。

使用此政策

您可以將 EC2InstanceConnect 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 6 月 27 日 18：53 UTC
- 編輯時間：2019 年 6 月 27 日 18：53 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceConnect

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

Ec2InstanceConnectEndpoint

描述：EC2 Instance Connect 端點政策，用於管理客戶建立的 EC2 Instance Connect 端點

`Ec2InstanceConnectEndpoint` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 1 月 24 日 20：19 UTC
- 編輯時間：2025 年 7 月 31 日 17：49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

EC2InstanceProfileForImageBuilder

描述：Image Builder 服務的 EC2 執行個體描述檔。

`EC2InstanceProfileForImageBuilder` 是 AWS 受管政策。

使用此政策

您可以將 `EC2InstanceProfileForImageBuilder` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 12 月 1 日 19：08 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot",
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*.ISO",
        "arn:aws:s3:::*/*.iso",
        "arn:aws:s3:::*/*.Iso"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetMarketplaceResource"
      ],
      "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/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

EC2InstanceProfileForImageBuilderECRContainerBuilds

描述：使用 EC2 Image Builder 建置容器映像的 EC2 執行個體描述檔。此政策授予使用者上傳 ECR 映像的廣泛許可。

EC2InstanceProfileForImageBuilderECRContainerBuilds 是 AWS 受管政策。

使用此政策

您可以將 EC2InstanceProfileForImageBuilderECRContainerBuilds 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 12 月 11 日 19：48 UTC
- 編輯時間：2020 年 12 月 11 日 19：48 UTC
- ARN: arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ECRReplicationServiceRolePolicy

描述：允許存取 AWS 服務 和 ECR 複寫使用或管理的資源

`ECRReplicationServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 4 日，22：11 UTC
- 編輯時間：2020 年 12 月 4 日，22：11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

ECRTemplateServiceRolePolicy

描述：允許在使用 AWS ECR 儲存庫建立範本時執行動作

ECRTemplateServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 6 月 19 日 23：11 UTC
- 編輯時間：2024 年 6 月 19 日 23：11 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateRepositoryWithTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ElastiCacheServiceRolePolicy

描述：此政策允許 ElastiCache 視需要代表您管理 AWS 資源，以管理您的快取

`ElastiCacheServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 12 月 7 日 17：50 UTC

- **編輯時間**：2023 年 11 月 28 日 03：05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

ElasticLoadBalancingFullAccess

描述：提供對 Amazon ElasticLoadBalancing 的完整存取權，以及對提供 ElasticLoadBalancing 功能所需的其他服務的有限存取權。

`ElasticLoadBalancingFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ElasticLoadBalancingFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 9 月 20 日，UTC 20：42
- 編輯時間：2026 年 2 月 23 日 18：57 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ElasticLoadBalancingReadOnly

描述：提供對 Amazon ElasticLoadBalancing 和相依服務的唯讀存取權

`ElasticLoadBalancingReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `ElasticLoadBalancingReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 9 月 20 日，UTC 20：17
- 編輯時間：2023 年 11 月 26 日 18：15 UTC

- ARN: arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ElementalActivationsDownloadSoftwareAccess

描述：檢視購買資產和下載相關軟體和入門檔案的存取權

`ElementalActivationsDownloadSoftwareAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ElementalActivationsDownloadSoftwareAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 9 月 8 日 17：26 UTC
- 編輯時間：2020 年 9 月 8 日 17：26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ElementalActivationsFullAccess

描述：檢視 Elemental Appliances and Software 購買資產並對其採取動作的完整存取權

`ElementalActivationsFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ElementalActivationsFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- 建立時間：2020 年 6 月 4 日，21：00 UTC
- 編輯時間：2020 年 6 月 4 日 21：00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ElementalActivationsGenerateLicenses

描述：檢視購買資產並產生軟體授權以進行待定啟用的存取權

`ElementalActivationsGenerateLicenses` 是 AWS 受管政策。

使用此政策

您可以將 ElementalActivationsGenerateLicenses 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 8 月 28 日 18：28 UTC
- 編輯時間：2020 年 8 月 28 日 18：28 UTC
- ARN: arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ElementalActivationsReadOnlyAccess

描述：唯讀存取與 AWS 帳戶 使用者 相關聯的已購買資產詳細清單

`ElementalActivationsReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ElementalActivationsReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 8 月 28 日 16：51 UTC
- 編輯時間：2020 年 8 月 28 日 16：51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ElementalAppliancesSoftwareFullAccess

描述：完整存取以檢視 Elemental Appliances 和 Software 引號和訂單並採取動作

`ElementalAppliancesSoftwareFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ElementalAppliancesSoftwareFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 7 月 31 日 16：28 UTC
- 編輯時間：2021 年 2 月 5 日 21：01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ElementalAppliancesSoftwareReadOnlyAccess

描述：檢視 Elemental Appliances and Software 引號和訂單的唯讀存取權

`ElementalAppliancesSoftwareReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ElementalAppliancesSoftwareReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2020 年 4 月 1 日，UTC 22：31
- 編輯時間：2020 年 4 月 1 日，22：31 UTC

- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ElementalSupportCenterFullAccess

描述：完整存取以檢視 Elemental Appliance and Software 支援案例和產品支援內容並採取動作

`ElementalSupportCenterFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 ElementalSupportCenterFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 11 月 25 日 18：08 UTC
- 編輯時間：2021 年 2 月 5 日 21：02 UTC
- ARN: arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

EMRDescribeClusterPolicyForEMRWAL

描述：此政策授予唯讀許可，允許 Amazon EMR 的 WAL 服務尋找並傳回叢集的狀態

EMRDescribeClusterPolicyForEMRWAL 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 6 月 15 日 23：30 UTC
- 編輯時間：2023 年 6 月 15 日 23：30 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

FMSServiceRolePolicy

描述：存取政策，以允許 FM 服務連結角色在客戶 AWS 組織帳戶中的 FM 受管資源上執行 FM 相關動作。

FMSServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 3 月 28 日，UTC 23：01
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy

政策版本

政策版本： v36 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WafGeneral",
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
```

```
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
    },
    {
      "Sid" : "WafWebaclCreation",
      "Effect" : "Allow",
      "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Sid" : "ElbGeneral",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WafPermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
```

```
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Sid" : "CloudfrontGeneral",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigScoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation",
        "config:DeleteEvaluationResults"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Sid" : "ConfigUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
```

```
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig",
        "config:BatchGetResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
    },
    {
      "Sid" : "OrganizationsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ShieldGeneral",
      "Effect" : "Allow",
      "Action" : [
```

```
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2SecurityGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SecurityGroupTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "SecurityGroupTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
      "Sid" : "Ec2Unscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Wafv2General",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "Wafv2WebAclAndRuleGroupMutation",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
```

```
      ]
    },
    {
      "Sid" : "Wafv2PermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid" : "Wafv2WebaclDescribe",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "RouteTableTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SubnetTagManagement",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RouteTableCleanup",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "Ec2DescribeUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateVpcEndpointScoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "CreateVpcEndpointUnscoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VpcEndpointsDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RamMutation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamCreation",
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "RamDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamDescribe",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "NetworkFirewallTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkFirewallGeneral",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListTLSInspectionConfigurations"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "NetworkFirewallResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:firewall-policy/*",
        "arn:aws:network-firewall:*:*:stateful-rulegroup/*",
        "arn:aws:network-firewall:*:*:stateless-rulegroup/*"
      ]
    },
    {
      "Sid" : "NetworkFirewallCleanup",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LogsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
```

```
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupCleanup",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ResolverRuleGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl"
        }
      }
    },
    {
      "Sid" : "NaclTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkAclEntry",
        "ec2:CreateNetworkAclEntry",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateNetworkAcl"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

FSxDeleteServiceLinkedRoleAccess

描述：允許 Amazon FSx 刪除其 Amazon S3 存取的服務連結角色

`FSxDeleteServiceLinkedRoleAccess` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 28 日 10：40 UTC
- 編輯時間：2018 年 11 月 28 日 10：40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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_*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

GameLiftContainerFleetPolicy

描述：授予 Amazon GameLift 容器機群中運算動作的必要許可，包括存取 Amazon S3 等相依性。

GameLiftContainerFleetPolicy 是 AWS 受管政策。

使用此政策

您可以將 GameLiftContainerFleetPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 12 日 19：28 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftContainerFleetPolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WriteGameSessionLogsToLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*:log-stream:*"
    },
    {
      "Sid" : "CreateLogGroupToStoreGameSessionLogs",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*"
    },
    {
      "Sid" : "WriteGameSessionLogsToS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
```

```
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::gamelift-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RetrieveComputeAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "gamelift:GetComputeAuthToken"
      ],
      "Resource" : [
        "arn:aws:gamelift:*:*:containerfleet/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

GameLiftGameServerGroupPolicy

描述：允許 Gamelift GameServerGroups 管理客戶資源的政策

`GameLiftGameServerGroupPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `GameLiftGameServerGroupPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 4 月 3 日，UTC 23：12
- 編輯時間：2020 年 5 月 13 日 17：27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- [在 IAM Identity Center 中使用 AWS 受管政策建立許可集]

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

GitLabDuoWithAmazonQPermissionsPolicy

描述：此受管政策授予與 Amazon Q 連線的許可，並利用 GitLab Duo 中的功能與 Amazon Q 整合。

GitLabDuoWithAmazonQPermissionsPolicy 是 AWS 受管政策。

使用此政策

您可以將 GitLabDuoWithAmazonQPermissionsPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 4 月 16 日 16：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/GitLabDuoWithAmazonQPermissionsPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GitLabDuoUsagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:SendEvent",
```

```
        "q:CreateAuthGrant",
        "q:UpdateAuthGrant",
        "q:GenerateCodeRecommendations",
        "q:SendMessage",
        "q:ListPlugins",
        "q:VerifyOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateOAuthAppConnection",
        "q:DeleteOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoPluginPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin"
      ],
      "Resource" : "arn:aws:qdeveloper:*:*:plugin/GitLabDuoWithAmazonQ/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

GlobalAcceleratorFullAccess

描述：允許 GlobalAccelerator 使用者完整存取所有 APIs

GlobalAcceleratorFullAccess 是 AWS 受管政策。

使用此政策

您可以將 GlobalAcceleratorFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 27 日 02：44 UTC
- 編輯時間：2020 年 12 月 4 日 19：17 UTC
- ARN: arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

GlobalAcceleratorReadOnlyAccess

描述：允許 GlobalAccelerator 使用者存取唯讀 APIs

`GlobalAcceleratorReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `GlobalAcceleratorReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 27 日 02：41 UTC
- 編輯時間：2018 年 11 月 27 日 02：41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

GreengrassOTAUpdateArtifactAccess

描述：提供所有 Greengrass 區域中 Greengrass OTA 更新成品的讀取存取權

`GreengrassOTAUpdateArtifactAccess` 是 AWS 受管政策。

使用此政策

您可以將 `GreengrassOTAUpdateArtifactAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 11 月 29 日 18：11 UTC
- 編輯時間：2018 年 12 月 18 日 00：59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
```

```
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

GroundTruthSyntheticConsoleFullAccess

描述：此政策授予使用 SageMaker Ground Truth Synthetic Console 所有功能所需的許可。

`GroundTruthSyntheticConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `GroundTruthSyntheticConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 8 月 25 日 15：58 UTC
- 編輯時間：2022 年 8 月 25 日 15：58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

GroundTruthSyntheticConsoleReadOnlyAccess

描述：此政策透過 授予對 SageMaker Ground Truth Synthetic 的唯讀存取權 AWS 管理主控台。

`GroundTruthSyntheticConsoleReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `GroundTruthSyntheticConsoleReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- **建立時間**：2022 年 8 月 25 日 15：58 UTC
- **編輯時間**：2022 年 8 月 25 日 15：58 UTC

- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

Health_OrganizationsServiceRolePolicy

描述：啟用組織檢視功能 AWS 的運作狀態政策

`Health_OrganizationsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 12 月 16 日 13：28 UTC
- 編輯時間：2024 年 2 月 6 日 16：07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

IAMAccessAdvisorReadOnly

描述：此政策授予讀取 IAM 存取顧問提供的所有存取資訊的存取權，例如服務上次存取的資訊。

IAMAccessAdvisorReadOnly 是 AWS 受管政策。

使用此政策

您可以將 IAMAccessAdvisorReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 6 月 21 日 19：33 UTC
- 編輯時間：2019 年 6 月 21 日 19：33 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

IAMAccessAnalyzerFullAccess

描述：提供 IAM Access Analyzer 的完整存取權

`IAMAccessAnalyzerFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 IAMAccessAnalyzerFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 12 月 2 日 17：12 UTC
- 編輯時間：2019 年 12 月 2 日 17：12 UTC
- ARN: arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

IAMAccessAnalyzerReadOnlyAccess

描述：提供 IAM Access Analyzer 資源的唯讀存取權

`IAMAccessAnalyzerReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `IAMAccessAnalyzerReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- **建立時間**：2019 年 12 月 2 日 17：12 UTC
- **編輯時間**：2024 年 7 月 18 日 17：49 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

IAMFullAccess

描述：透過 提供 IAM 的完整存取權 AWS 管理主控台。

IAMFullAccess 是 AWS 受管政策。

使用此政策

您可以將 IAMFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2019 年 6 月 21 日 19：40 UTC
- ARN: arn:aws:iam::aws:policy/IAMFullAccess

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

IAMReadOnlyAccess

描述：透過 提供 IAM 的唯讀存取權 AWS 管理主控台。

`IAMReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `IAMReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：40 UTC
- 編輯時間：2018 年 1 月 25 日 19：11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

IAMSelfManageServiceSpecificCredentials

描述：允許 IAM 使用者管理自己的服務特定登入資料。

`IAMSelfManageServiceSpecificCredentials` 是 AWS 受管政策。

使用此政策

您可以將 `IAMSelfManageServiceSpecificCredentials` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2016 年 12 月 22 日 17：25 UTC
- 編輯時間：2016 年 12 月 22 日 17：25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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}"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並邁向最低權限許可

IAMUserChangePassword

描述：讓 IAM 使用者能夠變更自己的密碼。

IAMUserChangePassword 是 AWS 受管政策。

使用此政策

您可以將 IAMUserChangePassword 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2016 年 11 月 15 日 00：25 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/IAMUserChangePassword

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:user/${aws:username}",
        "arn:aws:iam::*:user/*/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

IAMUserSSHKeys

描述：讓 IAM 使用者能夠管理自己的 SSH 金鑰。

`IAMUserSSHKeys` 是 AWS 受管政策。

使用此政策

您可以將 `IAMUserSSHKeys` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 7 月 9 日 17：08 UTC
- 編輯時間：2015 年 7 月 9 日 17：08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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}"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

IVSFullAccess

描述：提供互動式影片服務 (IVS) 的完整存取權，也包含相依服務的許可，完整存取 ivs 主控台所需的許可。

IVSFullAccess 是 AWS 受管政策。

使用此政策

您可以將 IVSFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 12 月 13 日 21：20 UTC
- 編輯時間：2023 年 12 月 13 日 21：20 UTC
- ARN: arn:aws:iam::aws:policy/IVSFullAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

IVSReadOnlyAccess

描述：提供對 IVS 低延遲和即時串流 APIs唯讀存取權

IVSReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 IVSReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 12 月 5 日 18：00 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: arn:aws:iam::aws:policy/IVSReadOnlyAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantReplicas",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

IVSRecordToS3

描述：執行 S3 PutObject 以記錄 IVS 即時串流的服務連結角色

IVSRecordToS3 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 12 月 5 日 00：10 UTC
- 編輯時間：2020 年 12 月 5 日 00：10 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

KafkaConnectServiceRolePolicy

描述：此政策授予 Kafka Connect 代表您管理 AWS 資源的許可。

KafkaConnectServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 9 月 7 日 13：12 UTC
- 編輯時間：2021 年 9 月 7 日 13：12 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

KafkaServiceRolePolicy

描述：Kafka 的 IAM 服務連結角色政策。

KafkaServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 11 月 15 日 23：31 UTC
- 編輯時間：2025 年 11 月 10 日 23：19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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_*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:*:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

KeyspacesCDCServiceRolePolicy

描述：授予 Amazon Keyspaces 變更資料擷取所需的許可

KeyspacesCDCServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 6 月 21 日 00：22 UTC
- 編輯時間：2025 年 6 月 21 日 00：22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KeyspacesCDCServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesPutMetricDataPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Cassandra"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

KeyspacesReplicationServiceRolePolicy

描述：Keyspaces 跨區域資料複寫所需的許可

KeyspacesReplicationServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 5 月 2 日 16：15 UTC
- 編輯時間：2024 年 11 月 15 日 20：55 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:Modify",
        "cassandra:Alter",
        "cassandra:ModifyMultiRegionResource",
        "cassandra:SelectMultiRegionResource",
        "cassandra:AlterMultiRegionResource",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWDeleteAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*"
    },
    {
      "Sid" : "CWDescribeAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
```

```
      "Sid" : "CWPutMetricAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "cloudwatch:AlarmActions" : [
            "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/cassandra/keyspace/*/
table/*:policyName/*:createdBy/*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

LakeFormationDataAccessServiceRolePolicy

描述：授予臨時資料存取 Lake Formation 資源的政策

`LakeFormationDataAccessServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 6 月 20 日 20：46 UTC
- 編輯時間：2024 年 2 月 6 日 18：37 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

LexBotPolicy

描述： AWS Lex Bot 使用案例的政策

`LexBotPolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 2 月 17 日 22：18 UTC
- 編輯時間：2019 年 11 月 13 日 22：29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

LexChannelPolicy

描述： AWS Lex 頻道使用案例的政策

LexChannelPolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2017 年 2 月 17 日 23：23 UTC
- 編輯時間：2017 年 2 月 17 日 23：23 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

LightsailExportAccess

描述： AWS Lightsail授予匯出資源許可的服務連結角色政策

`LightsailExportAccess` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 9 月 28 日 16：35 UTC
- 編輯時間：2022 年 1 月 15 日 01：45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

MediaConnectGatewayInstanceRolePolicy

描述：此政策授予將 MediaConnect Gateway 執行個體註冊到 MediaConnect Gateway 的許可。

`MediaConnectGatewayInstanceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `MediaConnectGatewayInstanceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 3 月 22 日 20：43 UTC
- 編輯時間：2023 年 3 月 22 日 20：43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

MediaPackageServiceRolePolicy

描述：允許 MediaPackage 將日誌發佈至 CloudWatch

`MediaPackageServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 9 月 18 日 17：45 UTC
- 編輯時間：2020 年 9 月 18 日 17：45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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/*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

MemoryDBServiceRolePolicy

描述：此政策允許 MemoryDB 視需要代表您管理 AWS 資源，以管理您的資源。

`MemoryDBServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- 建立時間：2021 年 8 月 17 日，UTC 22：34
- 編輯時間：2024 年 12 月 1 日 16：21 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateMemoryDBTagsOnNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonMemoryDBManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteMemoryDBTaggedNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "DescribeEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutCloudWatchMetricData",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MemoryDB"
        }
      }
    },
    {
      "Sid" : "ReplicateMemoryDBMultiRegionClusterData",
      "Effect" : "Allow",
      "Action" : [
        "memorydb:ReplicateMultiRegionClusterData"
      ],
      "Resource" : "arn:aws:memorydb:*:*:cluster/*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

MigrationHubDMSAccessServiceRolePolicy

描述： Database Migration Service 在客戶帳戶中擔任角色以呼叫 Migration Hub 的政策

`MigrationHubDMSAccessServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 6 月 12 日 17：50 UTC

- **編輯時間**：2019 年 10 月 7 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

MigrationHubServiceRolePolicy

描述：允許 Migration Hub 代表您呼叫 Application Discovery Service

`MigrationHubServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 6 月 12 日 17：22 UTC
- 編輯時間：2020 年 8 月 6 日 18：08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

MigrationHubSMSAccessServiceRolePolicy

描述： Server Migration Service 在客戶帳戶中擔任角色以呼叫 Migration Hub 的政策

`MigrationHubSMSAccessServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 6 月 12 日 18：30 UTC
- 編輯時間：2019 年 10 月 7 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

MonitronServiceRolePolicy

描述：授予必要客戶資源存取權之 AWS Monitron 服務連結角色的政策。

MonitronServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 5 月 2 日 19：22 UTC
- 編輯時間：2022 年 5 月 2 日 19：22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

MultiPartyApprovalFullAccess

描述：提供多方核准的完整存取權。此政策也包含 AWS Organizations 和 AWS IAM Identity 的相關許可，用於管理核准團隊和身分來源。

`MultiPartyApprovalFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `MultiPartyApprovalFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 6 月 18 日 20：22 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalFullAccess`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOCreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/mpa"
      ]
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
```

```
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "mpa.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:ListInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

MultiPartyApprovalReadOnlyAccess

描述：提供多方核准的唯讀存取權。此政策也包含核准團隊和身分來源對 AWS Organizations 和 AWS IAM Identity 的相關讀取許可。

`MultiPartyApprovalReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `MultiPartyApprovalReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 6 月 18 日 20：07 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC

- ARN: arn:aws:iam::aws:policy/MultiPartyApprovalReadOnlyAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:Get*",
        "mpa:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

NeptuneConsoleFullAccess

描述：提供使用 管理 Amazon Neptune 的完整存取權 AWS 管理主控台。請注意，此政策也授予帳戶內所有 SNS 主題發佈的完整存取權、建立和編輯 Amazon EC2 執行個體和 VPC 組態的許可、在 Amazon KMS 上檢視和列出金鑰的許可，以及 Amazon RDS 的完整存取權。如需詳細資訊，請參閱 https：//https://aws.amazon.com/neptune/faqs/。

`NeptuneConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `NeptuneConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 6 月 19 日，UTC 21：35
- 編輯時間：2023 年 11 月 30 日 07：32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "AllowOtherDepedentPermissions",
```

```
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

NeptuneFullAccess

描述：提供 Amazon Neptune 的完整存取權。請注意，此政策也會授予帳戶內所有 SNS 主題發佈的完整存取權，以及 Amazon RDS 的完整存取權。如需詳細資訊，請參閱 https：//https://aws.amazon.com/neptune/faqs/。

`NeptuneFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `NeptuneFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 5 月 30 日 19：17 UTC
- 編輯時間：2024 年 1 月 22 日 16：32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterEndpoint",
```

```
            "rds:CreateDBClusterParameterGroup",
            "rds:CreateDBClusterSnapshot",
            "rds:CreateDBParameterGroup",
            "rds:CreateDBSubnetGroup",
            "rds:CreateEventSubscription",
            "rds:CreateGlobalCluster",
            "rds:DeleteDBCluster",
            "rds:DeleteDBClusterEndpoint",
            "rds:DeleteDBClusterParameterGroup",
            "rds:DeleteDBClusterSnapshot",
            "rds:DeleteDBInstance",
            "rds:DeleteDBParameterGroup",
            "rds:DeleteDBSubnetGroup",
            "rds:DeleteEventSubscription",
            "rds:DeleteGlobalCluster",
            "rds:DescribeDBClusterEndpoints",
            "rds:DescribeAccountAttributes",
            "rds:DescribeCertificates",
            "rds:DescribeDBClusterParameterGroups",
            "rds:DescribeDBClusterParameters",
            "rds:DescribeDBClusterSnapshotAttributes",
            "rds:DescribeDBClusterSnapshots",
            "rds:DescribeDBClusters",
            "rds:DescribeDBEngineVersions",
            "rds:DescribeDBInstances",
            "rds:DescribeDBLogFiles",
            "rds:DescribeDBParameterGroups",
            "rds:DescribeDBParameters",
            "rds:DescribeDBSecurityGroups",
            "rds:DescribeDBSubnetGroups",
            "rds:DescribeEngineDefaultClusterParameters",
            "rds:DescribeEngineDefaultParameters",
            "rds:DescribeEventCategories",
            "rds:DescribeEventSubscriptions",
            "rds:DescribeEvents",
            "rds:DescribeGlobalClusters",
            "rds:DescribeOptionGroups",
            "rds:DescribeOrderableDBInstanceOptions",
            "rds:DescribePendingMaintenanceActions",
            "rds:DescribeValidDBInstanceModifications",
            "rds:DownloadDBLogFilePortion",
            "rds:FailoverDBCluster",
            "rds:FailoverGlobalCluster",
            "rds:ListTagsForResource",
```

```
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:StartDBCluster",
        "rds:StopDBCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

NeptuneGraphReadOnlyAccess

描述：提供所有 Amazon Neptune Analytics 資源的唯讀存取權，以及相依服務的唯讀許可。

`NeptuneGraphReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `NeptuneGraphReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 11 月 30 日 07：32 UTC
- 編輯時間：2023 年 11 月 30 日 07：32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

NeptuneReadOnlyAccess

描述：提供 Amazon Neptune 的唯讀存取權。請注意，此政策也會授予 Amazon RDS 資源的存取權。如需詳細資訊，請參閱 https：//https://aws.amazon.com/neptune/faqs/。

`NeptuneReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `NeptuneReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 5 月 30 日 19：16 UTC
- 編輯時間：2024 年 1 月 22 日 16：33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

NetworkAdministrator

描述：授予設定和設定 AWS 網路資源所需的 AWS 服務和動作的完整存取許可。

NetworkAdministrator 是 AWS 受管政策。

使用此政策

您可以將 NetworkAdministrator 連接至使用者、群組與角色。

政策詳細資訊

- 類型：任務函數政策
- 建立時間：2016 年 11 月 10 日 17：31 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/job-function/NetworkAdministrator

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDefaultNetworkAdminActions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
```

```
            "ec2:DescribeNatGateways",
            "ec2:DescribeNetworkAcls",
            "ec2:DescribeNetworkInterfaceAttribute",
            "ec2:DescribeNetworkInterfacePermissions",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribePlacementGroups",
            "ec2:DescribePrefixLists",
            "ec2:DescribePublicIpv4Pools",
            "ec2:DescribeRouteTables",
            "ec2:DescribeSecurityGroupReferences",
            "ec2:DescribeSecurityGroupRules",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeStaleSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeTags",
            "ec2:DescribeVpcAttribute",
            "ec2:DescribeVpcClassicLink",
            "ec2:DescribeVpcClassicLinkDnsSupport",
            "ec2:DescribeVpcEndpointConnectionNotifications",
            "ec2:DescribeVpcEndpointConnections",
            "ec2:DescribeVpcEndpointServiceConfigurations",
            "ec2:DescribeVpcEndpointServicePermissions",
            "ec2:DescribeVpcEndpointServices",
            "ec2:DescribeVpcEndpoints",
            "ec2:DescribeVpcPeeringConnections",
            "ec2:DescribeVpcs",
            "ec2:DescribeVpnConnections",
            "ec2:DescribeVpnGateways",
            "ec2:DetachInternetGateway",
            "ec2:DetachNetworkInterface",
            "ec2:DetachVpnGateway",
            "ec2:DisableVgwRoutePropagation",
            "ec2:DisableVpcClassicLinkDnsSupport",
            "ec2:DisassociateAddress",
            "ec2:DisassociateRouteTable",
            "ec2:DisassociateSubnetCidrBlock",
            "ec2:DisassociateVpcCidrBlock",
            "ec2:EnableVgwRoutePropagation",
            "ec2:EnableVpcClassicLinkDnsSupport",
            "ec2:GetVpnConnectionDeviceSampleConfiguration",
            "ec2:GetVpnConnectionDeviceTypes",
            "ec2:GetVpnTunnelReplacementStatus",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:ModifySecurityGroupRules",
```

```
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:ModifyVpnConnection",
        "ec2:ModifyVpnConnectionOptions",
        "ec2:ModifyVpnTunnelCertificate",
        "ec2:ModifyVpnTunnelOptions",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ReplaceVpnTunnel",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:*",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "route53:*",
        "route53domains:*",
        "sns:CreateTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowVPCPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AssociateSecurityGroupVpc",
        "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:DescribeSecurityGroupVpcAssociations",
        "ec2:DetachClassicLinkVpc",
        "ec2:DisableVpcClassicLink",
        "ec2:DisassociateSecurityGroupVpc",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowLocalGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLocalGatewayRoute",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteLocalGatewayRoute",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
```

```
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:SearchLocalGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DiscoverBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DiscoverFlowLogRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/flow-logs-*"
    },
    {
      "Sid" : "NetworkmanagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransitGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:CreateTransitGateway",
```

```
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ExportTransitGatewayRoutes",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTransitGatewaySLRCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

NetworkSecurityDirectorServiceLinkedRolePolicy

描述：提供 AWS Shield 網路安全主管服務連結角色的許可，以評估指定的環境。

NetworkSecurityDirectorServiceLinkedRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 6 月 13 日 20：07 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityDirectorServiceLinkedRolePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "ResourceLevelPermissionNotSupported",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "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:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetManagedPrefixListEntries",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "wafv2:ListWebACLs",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualInterfaces"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cloudfront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "classicWaf",
      "Effect" : "Allow",
      "Action" : [
        "waf:ListWebACLs",
        "waf:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*"
      ]
    },
    {
      "Sid" : "wafv2",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:GetRuleGroup",
        "wafv2:DescribeManagedRuleGroup",
        "wafv2:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/webacl/*/*",
        "arn:aws:wafv2:*:*:regional/webacl/*/*",
        "arn:aws:apprunner:*:*:service/*",
        "arn:aws:cognito-idp:*:*:userpool/*",
        "arn:aws:ec2:*:*:verified-access-instance/*"
```

```
      ]
    },
    {
      "Sid" : "directconnect",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways"
      ],
      "Resource" : [
        "arn:aws:directconnect::*:dx-gateway/*",
        "arn:aws:directconnect:*:*:dxcon/*",
        "arn:aws:directconnect:*:*:dxlag/*",
        "arn:aws:directconnect:*:*:dxvif/*"
      ]
    },
    {
      "Sid" : "ec2Get",
      "Effect" : "Allow",
      "Action" : [
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ]
    },
    {
      "Sid" : "networkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListFirewalls",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*/*"
      ]
    },
    {
```

```
      "Sid" : "apiGatewayGetAPI",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AllowOrganizationsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
```

```
            "network-security-director.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccountInformationRead",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderList",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

NovaActServiceRolePolicy

描述：此政策允許 NovaAct 建立和管理操作 Nova Act 代理程式所需的資源。

NovaActServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 11 月 26 日 16：19 UTC
- 編輯時間：2025 年 11 月 26 日 16：19 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/NovaActServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NovaAct"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

OAMFullAccess

描述：提供 CloudWatch Observability Access Manager 的完整存取權

`OAMFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `OAMFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2022 年 11 月 27 日 13：38 UTC
- 編輯時間：2022 年 11 月 27 日 13：38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

OAMReadOnlyAccess

描述：提供 CloudWatch Observability Access Manager 的唯讀存取權

`OAMReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `OAMReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 11 月 27 日 13：29 UTC
- 編輯時間：2022 年 11 月 27 日 13：29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

OpensearchIngestionSelfManagedVpcePolicy

描述：允許 Amazon OpenSearch Ingestion 描述網路資源，並將服務指標寫入 cloudwatch

`OpensearchIngestionSelfManagedVpcePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 6 月 10 日 19：59 UTC
- 編輯時間：2024 年 6 月 10 日 19：59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CwPermissionsForOsiNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
```

```
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

PartnerCentralAccountManagementUserRoleAssociation

描述：提供將合作夥伴中央使用者與 IAM 角色建立關聯和取消關聯的存取權

`PartnerCentralAccountManagementUserRoleAssociation` 是 AWS 受管政策。

使用此政策

您可以將 `PartnerCentralAccountManagementUserRoleAssociation` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 11 月 10 日 02：03 UTC
- 編輯時間：2023 年 11 月 10 日 02：03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

PartnerCentralIncentiveBenefitManagement

描述：政策提供管理 AWS Partner Central 中所有獎勵利益的存取權。

`PartnerCentralIncentiveBenefitManagement` 是 AWS 受管政策。

使用此政策

您可以將 PartnerCentralIncentiveBenefitManagement 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2026 年 2 月 11 日 16：42 UTC
- 編輯時間：2026 年 3 月 12 日 16：57 UTC
- ARN: arn:aws:iam::aws:policy/PartnerCentralIncentiveBenefitManagement

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BenefitsManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListBenefits",
        "partnercentral:GetBenefit",
        "partnercentral:CreateBenefitApplication",
        "partnercentral:AmendBenefitApplication",
        "partnercentral:UpdateBenefitApplication",
        "partnercentral:SubmitBenefitApplication",
        "partnercentral:GetBenefitApplication",
        "partnercentral:CancelBenefitApplication",
        "partnercentral:RecallBenefitApplication",
        "partnercentral:ListBenefitApplications",
        "partnercentral:AssociateBenefitApplicationResource",
        "partnercentral:DisassociateBenefitApplicationResource",
        "partnercentral:ListBenefitAllocations",
```

```
        "partnercentral:GetBenefitAllocation"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/benefit-application/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit-allocation/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralBenefitsTaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/benefit-application/*",
        "arn:aws:partnercentral:*:*:catalog/*/benefit-allocation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
```

```
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "AWSPartnerOpportunityAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetOpportunity",
        "partnercentral:ListOpportunities"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOffersAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
```

```
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "PartnerCentralAgentsSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:UseSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        },
        "Bool" : {
```

```
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

PowerUserAccess

描述：提供 AWS 服務和資源的完整存取權，但不允許管理使用者和群組。

PowerUserAccess 是 AWS 受管政策。

使用此政策

您可以將 PowerUserAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/PowerUserAccess

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:ListRegions",
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

QAppsServiceRolePolicy

描述：將許可授予 AWS 服務 Amazon Q 應用程式使用或管理的資源。

QAppsServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 9 月 26 日 19：22 UTC
- 編輯時間：2024 年 9 月 26 日 19：22 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/QAppsServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QAppsPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QApps"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

QBusinessQuicksightPluginPolicy

描述：授予許可給 QBusiness，以呼叫 QuickSight 外掛程式的 QuickSight APIs

`QBusinessQuicksightPluginPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `QBusinessQuicksightPluginPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 12 月 3 日 15：36 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/QBusinessQuicksightPluginPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PredictQAResults"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

QBusinessServiceRolePolicy

描述：授予許可給 AWS 服務 和 Amazon Q 使用或管理的資源

`QBusinessServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 4 月 29 日 16：05 UTC
- 編輯時間：2024 年 4 月 29 日 16：05 UTC

- ARN: arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QBusiness"
        }
      }
    },
    {
      "Sid" : "QBusinessCreateLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "QBusinessDescribeLogGroupsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QBusinessLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

描述：QuickSight 團隊用來存取 S3 Storage Management Analytics 產生之客戶資料的政策。

QuickSightAccessForS3StorageManagementAnalyticsReadOnly 是 AWS 受管政策。

使用此政策

您可以將 QuickSightAccessForS3StorageManagementAnalyticsReadOnly 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2017 年 6 月 12 日 18：18 UTC
- 編輯時間：2019 年 10 月 8 日 23：53 UTC
- ARN: arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

RDSCloudHsmAuthorizationRole

描述：Amazon RDS 服務角色的預設政策。

RDSCloudHsmAuthorizationRole 是 AWS 受管政策。

使用此政策

您可以將 RDSCloudHsmAuthorizationRole 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2019 年 9 月 26 日 22：14 UTC
- ARN: arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ReadOnlyAccess

描述：提供對 AWS 服務和資源的唯讀存取權。

`ReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

政策版本

政策版本： v178 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActionsGroup1",
      "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:GetFindingsStatistics",
        "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:GetContactInformation",
        "account:GetGovCloudAccountInformation",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "action-recommendations:ListRecommendedActions",
        "aiops:GetEphemeralInvestigationResults",
        "aiops:GetFact",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationEvent",
        "aiops:GetInvestigationGroup",
        "aiops:GetInvestigationResource",
        "aiops:GetReport",
        "aiops:ListFacts",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "aiops:ValidateInvestigationGroup",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBackendEnvironment",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:GetWebhook",
        "amplify:ListApps",
        "amplify:ListArtifacts",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "amplify:ListTagsForResource",
        "amplify:ListWebhooks",
```

```
            "aoss:BatchGetCollection",
            "aoss:BatchGetCollectionGroup",
            "aoss:BatchGetLifecyclePolicy",
            "aoss:BatchGetVpcEndpoint",
            "aoss:GetAccessPolicy",
            "aoss:GetAccountSettings",
            "aoss:GetPoliciesStats",
            "aoss:GetSecurityConfig",
            "aoss:GetSecurityPolicy",
            "aoss:ListAccessPolicies",
            "aoss:ListCollections",
            "aoss:ListCollectionGroups",
            "aoss:ListLifecyclePolicies",
            "aoss:ListSecurityConfigs",
            "aoss:ListSecurityPolicies",
            "aoss:ListTagsForResource",
            "aoss:ListVpcEndpoints",
            "apigateway:GET",
            "apigateway:GetPortal",
            "apigateway:GetPortalProduct",
            "apigateway:GetProductPage",
            "apigateway:GetProductRestEndpointPage",
            "apigateway:GetRoutingRule",
            "apigateway:ListPortalProducts",
            "apigateway:ListPortals",
            "apigateway:ListProductPages",
            "apigateway:ListProductRestEndpointPages",
            "apigateway:ListRoutingRules",
            "appconfig:GetApplication",
            "appconfig:GetConfiguration",
            "appconfig:GetConfigurationProfile",
            "appconfig:GetDeployment",
            "appconfig:GetDeploymentStrategy",
            "appconfig:GetEnvironment",
            "appconfig:GetExtension",
            "appconfig:GetHostedConfigurationVersion",
            "appconfig:ListApplications",
            "appconfig:ListConfigurationProfiles",
            "appconfig:ListDeployments",
            "appconfig:ListDeploymentStrategies",
            "appconfig:ListEnvironments",
            "appconfig:ListExtensions",
            "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:GetPredictiveScalingForecast",
        "application-autoscaling:ListTagsForResource",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListAuditFindings",
        "application-signals:ListEntityEvents",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListObservedEntities",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListServiceStates",
        "application-signals:ListTagsForResource",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "appmesh:Describe*",
```

```
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListServicesForAutoScalingConfiguration",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:Describe*",
        "appstream:List*",
        "appstudio:GetAccountStatus",
        "appstudio:GetEnablementJobStatus",
        "appsync:Get*",
        "appsync:List*",
        "apptest:GetTestCase",
        "apptest:GetTestConfiguration",
        "apptest:GetTestRunStep",
        "apptest:GetTestSuite",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "apptest:ListTestConfigurations",
        "apptest:ListTestRuns",
        "apptest:ListTestRunSteps",
        "apptest:ListTestRunTestCases",
        "apptest:ListTestSuites",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeWorkspace",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetDefaultScraperConfiguration",
        "aps:GetLabels",
```

```
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:QueryMetrics",
        "arc-region-switch:GetPlan",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
        "artifact:GetCustomerAgreement",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements",
        "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-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserSession",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetCodeInterpreterSession",
```

```
        "bedrock-agentcore:GetEvent",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetMemoryRecord",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetTokenVault",
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListBrowserSessions",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListCodeInterpreterSessions",
        "bedrock-agentcore:ListEvents",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListMemoryRecords",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock-agentcore:RetrieveMemoryRecords",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationJob",
```

```
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPrompt",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetResourcePolicy",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEnforcedGuardrailsConfiguration",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetResourcePolicy",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "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:ListTagsForResource",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCommitmentPurchaseAnalysis",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostComparisonDrivers",
        "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:ListCommitmentPurchaseAnalyses",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListCostCategoryResourceAssociations",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:List*",
        "chime:Get*",
        "chime:List*",
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms-ml:GetAudienceGenerationJob",
        "cleanrooms-ml:GetAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModelPolicy",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListAudienceExportJobs",
        "cleanrooms-ml:ListAudienceGenerationJobs",
        "cleanrooms-ml:ListAudienceModels",
        "cleanrooms-ml:ListConfiguredAudienceModels",
        "cleanrooms-ml:ListTagsForResource",
        "cleanrooms-ml:ListTrainingDatasets",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationChangeRequest",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
```

```
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedJob",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationChangeRequests",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListProtectedJobs",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "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:GetResourcePolicy",
            "cloudhsm:List*",
            "cloudsearch:Describe*",
            "cloudsearch:List*",
            "cloudtrail:Describe*",
            "cloudtrail:Get*",
            "cloudtrail:List*",
            "cloudtrail:LookupEvents",
            "cloudwatch:Describe*",
            "cloudwatch:GenerateQuery",
            "cloudwatch:GenerateQueryResultsSummary",
            "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*",
        "codewhisperer:ListProfiles",
        "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:GetIdleRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "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",
        "controlcatalog:GetControl",
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListControlMappings",
        "controlcatalog:ListControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEfficiencyMetrics",
        "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*",
            "datazone:GetAsset",
            "datazone:GetAssetType",
            "datazone:GetDataProduct",
            "datazone:GetDataSource",
            "datazone:GetDataSourceRun",
            "datazone:GetDomain",
            "datazone:GetDomainSharingPolicy",
            "datazone:GetDomainUnit",
            "datazone:GetEnvironment",
            "datazone:GetEnvironmentAction",
            "datazone:GetEnvironmentBlueprint",
            "datazone:GetEnvironmentBlueprintConfiguration",
            "datazone:GetEnvironmentProfile",
            "datazone:GetFormType",
            "datazone:GetGlossary",
            "datazone:GetGlossaryTerm",
            "datazone:GetGroupProfile",
            "datazone:GetLineageNode",
            "datazone:GetListing",
            "datazone:GetMetadataGenerationRun",
            "datazone:GetProject",
            "datazone:GetProjectProfile",
            "datazone:GetSubscription",
            "datazone:GetSubscriptionEligibility",
            "datazone:GetSubscriptionGrant",
            "datazone:GetSubscriptionRequestDetails",
            "datazone:GetSubscriptionTarget",
            "datazone:GetTimeSeriesDataPoint",
```

```
            "datazone:GetUserProfile",
            "datazone:ListAccountEnvironments",
            "datazone:ListAssetRevisions",
            "datazone:ListDataProductRevisions",
            "datazone:ListDataSourceRunActivities",
            "datazone:ListDataSourceRuns",
            "datazone:ListDataSources",
            "datazone:ListDomains",
            "datazone:ListDomainUnitsForParent",
            "datazone:ListEntityOwners",
            "datazone:ListEnvironmentActions",
            "datazone:ListEnvironmentBlueprintConfigurations",
            "datazone:ListEnvironmentBlueprintConfigurationSummaries",
            "datazone:ListEnvironmentBlueprints",
            "datazone:ListEnvironmentProfiles",
            "datazone:ListEnvironments",
            "datazone:ListGroupsForUser",
            "datazone:ListLineageNodeHistory",
            "datazone:ListNotifications",
            "datazone:ListPolicyGrants",
            "datazone:ListProjectMemberships",
            "datazone:ListProjectProfiles",
            "datazone:ListProjects",
            "datazone:ListSubscriptionGrants",
            "datazone:ListSubscriptionRequests",
            "datazone:ListSubscriptions",
            "datazone:ListSubscriptionTargets",
            "datazone:ListTagsForResource",
            "datazone:ListTimeSeriesDataPoints",
            "datazone:Search",
            "datazone:SearchGroupProfiles",
            "datazone:SearchListings",
            "datazone:SearchTypes",
            "datazone:SearchUserProfiles",
            "dax:BatchGetItem",
            "dax:Describe*",
            "dax:GetItem",
            "dax:ListTags",
            "dax:Query",
            "dax:Scan",
            "deadline:BatchGetJobEntity",
            "deadline:GetApplicationVersion",
            "deadline:GetBudget",
            "deadline:GetFarm",
```

```
            "deadline:GetFleet",
            "deadline:GetJob",
            "deadline:GetLicenseEndpoint",
            "deadline:GetMonitor",
            "deadline:GetQueue",
            "deadline:GetQueueEnvironment",
            "deadline:GetQueueFleetAssociation",
            "deadline:GetSession",
            "deadline:GetSessionAction",
            "deadline:GetSessionsStatisticsAggregation",
            "deadline:GetStep",
            "deadline:GetStorageProfile",
            "deadline:GetStorageProfileForQueue",
            "deadline:GetTask",
            "deadline:GetWorker",
            "deadline:ListAvailableMeteredProducts",
            "deadline:ListBudgets",
            "deadline:ListFarmMembers",
            "deadline:ListFarms",
            "deadline:ListFleetMembers",
            "deadline:ListFleets",
            "deadline:ListJobMembers",
            "deadline:ListJobParameterDefinitions",
            "deadline:ListJobs",
            "deadline:ListLicenseEndpoints",
            "deadline:ListMeteredProducts",
            "deadline:ListMonitors",
            "deadline:ListQueueEnvironments",
            "deadline:ListQueueFleetAssociations",
            "deadline:ListQueueMembers",
            "deadline:ListQueues",
            "deadline:ListSessionActions",
            "deadline:ListSessions",
            "deadline:ListSessionsForWorker",
            "deadline:ListStepConsumers",
            "deadline:ListStepDependencies",
            "deadline:ListSteps",
            "deadline:ListStorageProfiles",
            "deadline:ListStorageProfilesForQueue",
            "deadline:ListTagsForResource",
            "deadline:ListTasks",
            "deadline:ListWorkers",
            "deadline:SearchJobs",
            "deadline:SearchSteps",
```

```
        "deadline:SearchTasks",
        "deadline:SearchWorkers",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
```

```
        "dms:Describe*",
        "dms:List*",
        "dms:Test*",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ListTagsForResource",
        "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*",
        "dsql:GetCluster",
        "dsql:GetClusterPolicy",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:BatchGet*",
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "ec2:Describe*",
        "ec2:DescribeInstanceImageMetadata",
        "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*",
        "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:GetAdminScope",
        "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:GetAccountActivity",
        "freetier:GetAccountPlanState",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:ListAccountActivities",
        "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:BatchGetTableOptimizer",
        "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:GetSession",
            "glue:GetStatement",
            "glue:GetTable",
            "glue:GetTableOptimizer",
            "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:ListSessions",
            "glue:ListStatements",
            "glue:ListTableOptimizerRuns",
            "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:BatchGetCodeSnippet",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:BatchGetMemberEc2DeepInspectionStatus",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetCisScanReport",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetEc2DeepInspectionConfiguration",
        "inspector2:GetEncryptionKey",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:GetSbomExport",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCisScanConfigurations",
        "inspector2:ListCisScans",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "inspector2:SearchVulnerabilities",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
```

```
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModels",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectors",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetLoggingOptions",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetRegisterAccountStatus",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
```

```
        "iotfleetwise:GetVehicleStatus",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMetricConfiguration",
        "iotwireless:GetMetrics",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
```

```
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
        "iotwireless:ListQueuedMessages",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipantEvents",
        "ivs:ListParticipants",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
```

```
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyActionsGroup2",
      "Effect" : "Allow",
      "Action" : [
        "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:ListDataSourceSyncJobs",
            "kendra:ListDataSources",
            "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:GetWorkloadDeploymentPattern",
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListTagsForResource",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:Get*",
        "lex:ListBotAliasReplicas",
```

```
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBotReplicas",
        "lex:ListBotVersionReplicas",
        "lex:ListBotVersions",
        "lex:ListBots",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListSlotTypes",
        "lex:ListSlots",
        "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:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDisks",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
```

```
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetLoadBalancers",
        "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:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAnomalies",
        "logs:ListEntitiesForLogGroup",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
```

```
        "logs:StartLiveTail",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:ListAggregateLogGroupSummaries",
        "logs:ListSourcesForS3TableIntegration",
        "logs:ListScheduledQueries",
        "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:ListModelVersions",
        "lookoutequipment:ListModels",
        "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:ListApplicationVersions",
        "m2:ListApplications",
        "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:GetFindingStatistics",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "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:ListProposalVotes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:GetRouterInput",
        "mediaconnect:GetRouterNetworkInterface",
        "mediaconnect:GetRouterOutput",
        "mediaconnect:ListBridges",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListTagsForResource",
```

```
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Probe",
        "mediaconvert:SearchJobs",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "medialive:DescribeAccountConfiguration",
        "medialive:DescribeChannel",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeCluster",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNetwork",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannels",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
```

```
            "mediapackagev2:GetChannelGroup",
            "mediapackagev2:GetChannelPolicy",
            "mediapackagev2:GetHeadObject",
            "mediapackagev2:GetObject",
            "mediapackagev2:GetOriginEndpoint",
            "mediapackagev2:GetOriginEndpointPolicy",
            "mediapackagev2:ListChannelGroups",
            "mediapackagev2:ListChannels",
            "mediapackagev2:ListOriginEndpoints",
            "mediapackagev2:ListTagsForResource",
            "mediastore:DescribeContainer",
            "mediastore:DescribeObject",
            "mediastore:GetContainerPolicy",
            "mediastore:GetCorsPolicy",
            "mediastore:GetLifecyclePolicy",
            "mediastore:GetMetricPolicy",
            "mediastore:GetObject",
            "mediastore:ListContainers",
            "mediastore:ListItems",
            "mediastore:ListTagsForResource",
            "memorydb:DescribeAcls",
            "memorydb:DescribeClusters",
            "memorydb:DescribeEngineVersions",
            "memorydb:DescribeEvents",
            "memorydb:DescribeMultiRegionClusters",
            "memorydb:DescribeMultiRegionParameterGroups",
            "memorydb:DescribeMultiRegionParameters",
            "memorydb:DescribeParameterGroups",
            "memorydb:DescribeParameters",
            "memorydb:DescribeReservedNodes",
            "memorydb:DescribeReservedNodesOfferings",
            "memorydb:DescribeServiceUpdates",
            "memorydb:DescribeSnapshots",
            "memorydb:DescribeSubnetGroups",
            "memorydb:DescribeUsers",
            "memorydb:ListAllowedMultiRegionClusterUpdates",
            "memorydb:ListAllowedNodeTypeUpdates",
            "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",
        "mpa:GetApprovalTeam",
        "mpa:GetIdentitySource",
        "mpa:GetPolicyVersion",
        "mpa:GetResourcePolicy",
        "mpa:GetSession",
        "mpa:ListApprovalTeams",
        "mpa:ListIdentitySources",
        "mpa:ListPolicies",
        "mpa:ListPolicyVersions",
        "mpa:ListResourcePolicies",
        "mpa:ListSessions",
        "mpa:ListTagsForResource",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeProxy",
        "network-firewall:DescribeProxyConfiguration",
        "network-firewall:DescribeProxyRule",
        "network-firewall:DescribeProxyRuleGroup",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListProxies",
```

```
        "network-firewall:ListProxyConfigurations",
        "network-firewall:ListProxyRuleGroups",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "networkflowmonitor:GetMonitor",
        "networkflowmonitor:GetScope",
        "networkflowmonitor:ListMonitors",
        "networkflowmonitor:ListScopes",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetConnections",
        "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:GetSiteToSiteVpnAttachment",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListAttachmentRoutingPolicyAssociations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworkPrefixListAssociations",
        "networkmanager:ListCoreNetworkRoutingInformation",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
```

```
        "networkmanager:ListTagsForResource",
        "networkmonitor:GetMonitor",
        "networkmonitor:GetProbe",
        "networkmonitor:ListMonitors",
        "networkmonitor: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:GetFeatureOptInStatus",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
```

```
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetS3TableIntegration",
        "omics:Get*",
        "omics:List*",
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
        "osis:GetPipelineChangeProgress",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
```

```
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "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:ListEnvironmentTemplates",
            "proton:ListEnvironments",
            "proton:ListServiceInstances",
            "proton:ListServiceTemplates",
            "proton:ListServices",
            "proton:ListTagsForResource",
            "purchase-orders:GetPurchaseOrder",
            "purchase-orders:ListPurchaseOrderInvoices",
            "purchase-orders:ListPurchaseOrders",
            "purchase-orders:ViewPurchaseOrders",
            "qbusiness:GetApplication",
            "qbusiness:GetChatControlsConfiguration",
            "qbusiness:GetDataSource",
            "qbusiness:GetGroup",
            "qbusiness:GetIndex",
            "qbusiness:GetPlugin",
            "qbusiness:GetRetriever",
            "qbusiness:GetUser",
            "qbusiness:GetWebExperience",
            "qbusiness:ListApplications",
            "qbusiness:ListDataSourceSyncJobs",
            "qbusiness:ListDataSources",
```

```
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift-serverless:GetCustomDomainAssociation",
        "redshift-serverless:GetEndpointAccess",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetRecoveryPoint",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:GetScheduledAction",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetTableRestoreStatus",
        "redshift-serverless:GetUsageLimit",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListCustomDomainAssociations",
        "redshift-serverless:ListEndpointAccess",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListRecoveryPoints",
        "redshift-serverless:ListScheduledActions",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTableRestoreStatus",
```

```
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListUsageLimits",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:ListRecommendations",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeProjects",
        "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:DescribeMetricsExport",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:DescribeResourceGroupingRecommendationTask",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessmentResourceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListApps",
        "resiliencehub:ListMetrics",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListResourceGroupingRecommendations",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetResourceExplorerSetup",
        "resource-explorer-2:GetServiceIndex",
        "resource-explorer-2:GetServiceView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListServiceIndexes",
        "resource-explorer-2:ListServiceViews",
        "resource-explorer-2:ListStreamingAccessForServices",
        "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*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
```

```
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetBucketVersioning",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:GetObject",
        "s3-outposts:GetObjectTagging",
        "s3-outposts:GetObjectVersion",
        "s3-outposts:GetObjectVersionForReplication",
        "s3-outposts:GetObjectVersionTagging",
        "s3-outposts:GetReplicationConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListBucket",
        "s3-outposts:ListBucketMultipartUploads",
        "s3-outposts:ListBucketVersions",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListMultipartUploadParts",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListRegionalBuckets",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:GetVectors",
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
```

```
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableData",
        "s3tables:GetTableEncryption",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTableMaintenanceJobStatus",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableRecordExpirationConfiguration",
        "s3tables:GetTableRecordExpirationJobStatus",
        "s3tables:GetTableReplication",
        "s3tables:GetTableReplicationStatus",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3tables:GetNamespace",
        "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:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "securitylake:GetDataLakeExceptionSubscription",
        "securitylake:GetDataLakeOrganizationConfiguration",
        "securitylake:GetDataLakeSources",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAutoManagementConfiguration",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetQuotaUtilizationReport",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
```

```
        "servicequotas:StartQuotaUtilizationReport",
        "ses:BatchGetMetricData",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "signer:DescribeSigningJob",
        "signer:GetSigningPlatform",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningJobs",
        "signer:ListSigningPlatforms",
        "signer:ListSigningProfiles",
        "signer:ListTagsForResource",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeRegistrationAttachments",
        "sms-voice:DescribeRegistrationFieldDefinitions",
        "sms-voice:DescribeRegistrationFieldValues",
        "sms-voice:DescribeRegistrations",
        "sms-voice:DescribeRegistrationSectionDefinitions",
        "sms-voice:DescribeRegistrationTypeDefinitions",
        "sms-voice:DescribeRegistrationVersions",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "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-quicksetup:GetConfiguration",
            "ssm-quicksetup:GetConfigurationManager",
            "ssm-quicksetup:GetServiceSettings",
            "ssm-quicksetup:ListConfigurationManagers",
            "ssm-quicksetup:ListConfigurations",
            "ssm-quicksetup:ListQuickSetupTypes",
            "ssm-quicksetup:ListTagsForResource",
            "ssm-sap:GetApplication",
            "ssm-sap:GetComponent",
            "ssm-sap:GetConfigurationCheckOperation",
            "ssm-sap:GetDatabase",
            "ssm-sap:GetOperation",
            "ssm-sap:GetResourcePermission",
            "ssm-sap:ListApplications",
            "ssm-sap:ListComponents",
            "ssm-sap:ListConfigurationCheckDefinitions",
            "ssm-sap:ListConfigurationCheckOperations",
            "ssm-sap:ListDatabases",
            "ssm-sap:ListOperationEvents",
            "ssm-sap:ListOperations",
```

```
        "ssm-sap:ListSubCheckResults",
        "ssm-sap:ListSubCheckRuleResults",
        "ssm-sap:ListTagsForResource",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "states:ValidateStateMachineDefinition",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunication",
        "support:DescribeCommunications",
        "support:DescribeCreateCaseOptions",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:DescribeSupportedLanguages",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorChecks",
        "support:SearchForCases",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "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",
        "transform-custom:GetCampaign",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:ListKnowledgeItems",
```

```
        "transform-custom:ListTagsForResource",
        "transform-custom:ListTransformationPackageMetadata",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "trustedadvisor:GetOrganizationRecommendation",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListOrganizationRecommendationAccounts",
        "trustedadvisor:ListOrganizationRecommendationResources",
        "trustedadvisor:ListOrganizationRecommendations",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
        "user-subscriptions:ListApplicationClaims",
        "user-subscriptions:ListClaims",
        "user-subscriptions:ListUserSubscriptions",
        "uxc:GetAccountColor",
        "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:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
```

```
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceEndpointAssociations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkVpcEndpointAssociations",
        "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:List*",
        "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:CancelTraceRetrieval",
        "xray:Get*",
        "xray:ListResourcePolicies",
        "xray:ListRetrievedTraces",
        "xray:ListTagsForResource",
        "xray:StartTraceRetrieval"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

ResourceGroupsandTagEditorFullAccess

描述：提供資源群組和標籤編輯器的完整存取權。

ResourceGroupsandTagEditorFullAccess 是 AWS 受管政策。

使用此政策

您可以將 ResourceGroupsandTagEditorFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2023 年 8 月 10 日 13：29 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ResourceGroupsandTagEditorReadOnlyAccess

描述：提供使用資源群組和標籤編輯器的存取權，但不允許透過標籤編輯器編輯標籤。

`ResourceGroupsandTagEditorReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ResourceGroupsandTagEditorReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：39 UTC
- 編輯時間：2023 年 8 月 10 日 13：42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ResourceGroupsServiceRolePolicy

描述：允許 AWS 資源群組查詢擁有您資源 AWS 的服務，讓群組保持up-to-date

`ResourceGroupsServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2023 年 1 月 5 日 16：57 UTC
- 編輯時間：2023 年 1 月 5 日 16：57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ResourceGroupsTaggingAPITagUntagSupportedResources

描述：提供許可，以標記和取消標記資源群組標記 API 支援的所有資源。此政策也會授予透過資源群組標記 API 擷取所有已標記或先前已標記之資源所需的許可。

ResourceGroupsTaggingAPITagUntagSupportedResources 是 AWS 受管政策。

使用此政策

您可以將 ResourceGroupsTaggingAPITagUntagSupportedResources 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 10 月 11 日 11：11 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/ResourceGroupsTaggingAPITagUntagSupportedResources

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:TagResource",
        "a4b:UntagResource",
        "access-analyzer:TagResource",
        "access-analyzer:UntagResource",
        "acm-pca:TagCertificateAuthority",
```

```
        "acm-pca:UntagCertificateAuthority",
        "acm:AddTagsToCertificate",
        "acm:RemoveTagsFromCertificate",
        "amplify:TagResource",
        "amplify:UntagResource",
        "appconfig:TagResource",
        "appconfig:UntagResource",
        "appflow:TagResource",
        "appflow:UntagResource",
        "appmesh:TagResource",
        "appmesh:UntagResource",
        "appstream:TagResource",
        "appstream:UntagResource",
        "appsync:TagResource",
        "appsync:UntagResource",
        "athena:TagResource",
        "athena:UntagResource",
        "auditmanager:TagResource",
        "auditmanager:UntagResource",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteTags",
        "backup:TagResource",
        "backup:UntagResource",
        "batch:TagResource",
        "batch:UntagResource",
        "braket:TagResource",
        "braket:UntagResource",
        "cassandra:TagResource",
        "cassandra:UntagResource",
        "chime:TagResource",
        "chime:UntagResource",
        "cloud9:TagResource",
        "cloud9:UntagResource",
        "clouddirectory:TagResource",
        "clouddirectory:UntagResource",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudhsm:TagResource",
        "cloudhsm:UntagResource",
        "cloudtrail:AddTags",
        "cloudtrail:RemoveTags",
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "codeartifact:TagResource",
```

```
        "codeartifact:UntagResource",
        "codecommit:TagResource",
        "codecommit:UntagResource",
        "codedeploy:AddTagsToOnPremisesInstances",
        "codedeploy:RemoveTagsFromOnPremisesInstances",
        "codedeploy:TagResource",
        "codedeploy:UntagResource",
        "codeguru-profiler:TagResource",
        "codeguru-profiler:UntagResource",
        "codepipeline:TagResource",
        "codepipeline:UntagResource",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar:TagProject",
        "codestar:UntagProject",
        "cognito-identity:TagResource",
        "cognito-identity:UntagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UntagResource",
        "comprehend:TagResource",
        "comprehend:UntagResource",
        "config:TagResource",
        "config:UntagResource",
        "connect:TagResource",
        "connect:UntagResource",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "datapipeline:AddTags",
        "datapipeline:RemoveTags",
        "datasync:TagResource",
        "datasync:UntagResource",
        "deepcomposer:TagResource",
        "deepcomposer:UntagResource",
        "detective:TagResource",
        "detective:UntagResource",
        "devicefarm:TagResource",
        "devicefarm:UntagResource",
        "directconnect:TagResource",
        "directconnect:UntagResource",
        "dlm:TagResource",
        "dlm:UntagResource",
        "dms:AddTagsToResource",
        "dms:RemoveTagsFromResource",
        "dynamodb:TagResource",
```

```
        "dynamodb:UntagResource",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ecr:TagResource",
        "ecr:UntagResource",
        "ecs:TagResource",
        "ecs:UntagResource",
        "eks:TagResource",
        "eks:UntagResource",
        "elastic-inference:TagResource",
        "elastic-inference:UntagResource",
        "elasticache:AddTagsToResource",
        "elasticache:RemoveTagsFromResource",
        "elasticbeanstalk:UpdateTagsForResource",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:DeleteTags",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "emr-containers:TagResource",
        "emr-containers:UntagResource",
        "es:AddTags",
        "es:RemoveTags",
        "events:TagResource",
        "events:UntagResource",
        "firehose:TagDeliveryStream",
        "firehose:UntagDeliveryStream",
        "fms:TagResource",
        "fms:UntagResource",
        "forecast:TagResource",
        "forecast:UntagResource",
        "frauddetector:TagResource",
        "frauddetector:UntagResource",
        "fsx:TagResource",
        "fsx:UntagResource",
        "gamelift:TagResource",
        "gamelift:UntagResource",
        "glacier:AddTagsToVault",
        "glacier:RemoveTagsFromVault",
        "globalaccelerator:TagResource",
        "globalaccelerator:UntagResource",
        "glue:TagResource",
        "glue:UntagResource",
```

```
            "greengrass:TagResource",
            "greengrass:UntagResource",
            "groundstation:TagResource",
            "groundstation:UntagResource",
            "guardduty:TagResource",
            "guardduty:UntagResource",
            "iam:TagInstanceProfile",
            "iam:TagMFADevice",
            "iam:TagOpenIDConnectProvider",
            "iam:TagPolicy",
            "iam:TagRole",
            "iam:TagSAMLProvider",
            "iam:TagServerCertificate",
            "iam:TagUser",
            "iam:UntagInstanceProfile",
            "iam:UntagMFADevice",
            "iam:UntagOpenIDConnectProvider",
            "iam:UntagPolicy",
            "iam:UntagRole",
            "iam:UntagSAMLProvider",
            "iam:UntagServerCertificate",
            "iam:UntagUser",
            "imagebuilder:TagResource",
            "imagebuilder:UntagResource",
            "inspector:ListTagsForResource",
            "inspector:SetTagsForResource",
            "iot1click:TagResource",
            "iot1click:UntagResource",
            "iot:TagResource",
            "iot:UntagResource",
            "iotanalytics:TagResource",
            "iotanalytics:UntagResource",
            "iotdeviceadvisor:TagResource",
            "iotdeviceadvisor:UntagResource",
            "iotevents:TagResource",
            "iotevents:UntagResource",
            "iotfleethub:TagResource",
            "iotfleethub:UntagResource",
            "iotsitewise:TagResource",
            "iotsitewise:UntagResource",
            "iottwinmaker:TagResource",
            "iottwinmaker:UntagResource",
            "iotwireless:TagResource",
            "iotwireless:UntagResource",
```

```
        "ivs:TagResource",
        "ivs:UntagResource",
        "kafka:TagResource",
        "kafka:UntagResource",
        "kendra:TagResource",
        "kendra:UntagResource",
        "kinesis:AddTagsToStream",
        "kinesis:RemoveTagsFromStream",
        "kinesisanalytics:TagResource",
        "kinesisanalytics:UntagResource",
        "kms:TagResource",
        "kms:UntagResource",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lex:TagResource",
        "lex:UntagResource",
        "license-manager:TagResource",
        "license-manager:UntagResource",
        "lightsail:TagResource",
        "lightsail:UntagResource",
        "logs:TagLogGroup",
        "logs:TagResource",
        "logs:UntagLogGroup",
        "logs:UntagResource",
        "lookoutequipment:TagResource",
        "lookoutequipment:UntagResource",
        "machinelearning:AddTags",
        "machinelearning:DeleteTags",
        "macie2:TagResource",
        "macie2:UntagResource",
        "managedblockchain:TagResource",
        "managedblockchain:UntagResource",
        "mediaconnect:TagResource",
        "mediaconnect:UntagResource",
        "mediaconvert:TagResource",
        "mediaconvert:UntagResource",
        "medialive:CreateTags",
        "medialive:DeleteTags",
        "mediapackage-vod:TagResource",
        "mediapackage-vod:UntagResource",
        "mediapackage:TagResource",
        "mediapackage:UntagResource",
        "mediatailor:TagResource",
        "mediatailor:UntagResource",
```

```
            "mobiletargeting:TagResource",
            "mobiletargeting:UntagResource",
            "mq:CreateTags",
            "mq:DeleteTags",
            "neptune-graph:TagResource",
            "neptune-graph:UntagResource",
            "network-firewall:TagResource",
            "network-firewall:UntagResource",
            "networkmanager:TagResource",
            "networkmanager:UntagResource",
            "opsworks-cm:TagResource",
            "opsworks-cm:UntagResource",
            "opsworks:TagResource",
            "opsworks:UntagResource",
            "organizations:TagResource",
            "organizations:UntagResource",
            "outposts:TagResource",
            "outposts:UntagResource",
            "qldb:TagResource",
            "qldb:UntagResource",
            "quicksight:TagResource",
            "quicksight:UntagResource",
            "ram:TagResource",
            "ram:UntagResource",
            "rds:AddTagsToResource",
            "rds:RemoveTagsFromResource",
            "redshift:CreateTags",
            "redshift:DeleteTags",
            "resource-explorer-2:TagResource",
            "resource-explorer-2:UntagResource",
            "resource-groups:Tag",
            "resource-groups:Untag",
            "robomaker:TagResource",
            "robomaker:UntagResource",
            "route53:ChangeTagsForResource",
            "route53domains:DeleteTagsForDomain",
            "route53domains:UpdateTagsForDomain",
            "route53resolver:TagResource",
            "route53resolver:UntagResource",
            "s3:GetBucketTagging",
            "s3:GetJobTagging",
            "s3:GetObjectTagging",
            "s3:GetObjectVersionTagging",
            "s3:GetStorageLensConfigurationTagging",
```

```
            "s3:DeleteJobTagging",
            "s3:DeleteObjectTagging",
            "s3:DeleteObjectVersionTagging",
            "s3:PutBucketTagging",
            "s3:PutJobTagging",
            "s3:PutObjectTagging",
            "s3:PutObjectVersionTagging",
            "s3:PutStorageLensConfigurationTagging",
            "s3:DeleteStorageLensConfigurationTagging",
            "s3:TagResource",
            "s3:UntagResource",
            "sagemaker:AddTags",
            "sagemaker:DeleteTags",
            "savingsplans:TagResource",
            "savingsplans:UntagResource",
            "schemas:TagResource",
            "schemas:UntagResource",
            "secretsmanager:TagResource",
            "secretsmanager:UntagResource",
            "securityhub:TagResource",
            "securityhub:UntagResource",
            "servicediscovery:TagResource",
            "servicediscovery:UntagResource",
            "servicequotas:TagResource",
            "servicequotas:UntagResource",
            "ses:TagResource",
            "ses:UntagResource",
            "sns:TagResource",
            "sns:UntagResource",
            "sqs:TagQueue",
            "sqs:UntagQueue",
            "ssm:AddTagsToResource",
            "ssm:RemoveTagsFromResource",
            "states:TagResource",
            "states:UntagResource",
            "storagegateway:AddTagsToResource",
            "storagegateway:RemoveTagsFromResource",
            "swf:TagResource",
            "swf:UntagResource",
            "synthetics:TagResource",
            "synthetics:UntagResource",
            "tag:GetResources",
            "tag:TagResources",
            "tag:UntagResources",
```

```
        "transfer:TagResource",
        "transfer:UntagResource",
        "waf-regional:TagResource",
        "waf-regional:UntagResource",
        "waf:TagResource",
        "waf:UntagResource",
        "wafv2:TagResource",
        "wafv2:UntagResource",
        "worklink:TagResource",
        "worklink:UntagResource",
        "workmail:TagResource",
        "workmail:UntagResource",
        "workspaces:CreateTags",
        "workspaces:DeleteTags",
        "xray:TagResource",
        "xray:UntagResource",
        "kinesisvideo:TagResource",
        "kinesisvideo:UntagResource",
        "redshift-serverless:TagResource",
        "redshift-serverless:UntagResource",
        "route53-recovery-control-config:TagResource",
        "route53-recovery-control-config:UntagResource",
        "route53-recovery-readiness:TagResource",
        "route53-recovery-readiness:UntagResource",
        "ssm-contacts:TagResource",
        "ssm-contacts:UntagResource",
        "ssm-incidents:TagResource",
        "ssm-incidents:UntagResource",
        "vpc-lattice:TagResource",
        "vpc-lattice:UntagResource",
        "workspaces-web:TagResource",
        "workspaces-web:UntagResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ROSAAmazonEBSCSIDriverOperatorPolicy

描述：允許 OpenShift Amazon EBS 容器儲存介面 (CSI) 驅動程式運算子在 Red Hat OpenShift Service on(ROSA) 叢集上安裝和維護 Amazon EBS CSI 驅動程式。 AWS Amazon EBS CSI 驅動程式可讓 ROSA 叢集管理持久性磁碟區的 Amazon EBS 磁碟區的生命週期。

`ROSAAmazonEBSCSIDriverOperatorPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSAAmazonEBSCSIDriverOperatorPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 4 月 20 日 22：36 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "CreateVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ROSACloudNetworkConfigOperatorPolicy

描述：允許 OpenShift Cloud Network Config Controller Operator 佈建和管理聯網資源，以供 Red Hat OpenShift Service on AWS (ROSA) 叢集聯網浮水印使用。OpenShift Cloud Network Operator 會透過 CustomResourceDefinitions 代表網路外掛程式與 AWS APIs 互動。 CustomResourceDefinitions 作為 ROSA 叢集的一部分，運算子會使用這些政策許可來管理 Amazon EC2 執行個體的私有 IP 地址。

`ROSACloudNetworkConfigOperatorPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSACloudNetworkConfigOperatorPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 4 月 20 日，UTC 22：34
- 編輯時間：2023 年 4 月 20 日，UTC 22：34
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ROSAControlPlaneOperatorPolicy

描述：允許 Red Hat OpenShift Service on AWS (ROSA) 控制平面管理 ROSA 叢集 Amazon EC2 和 Amazon Route 53 資源。

ROSAControlPlaneOperatorPolicy 是 AWS 受管政策。

使用此政策

您可以將 ROSAControlPlaneOperatorPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 4 月 24 日 23：02 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ROSAImageRegistryOperatorPolicy

描述：允許 OpenShift Image Registry Operator 佈建和管理 Amazon S3 儲存貯體和物件，供 Red Hat OpenShift Service on AWS (ROSA) 叢集內映像登錄檔使用，以滿足 ROSA 儲存需求。OpenShift Image Registry Operator 會安裝和維護 Red Hat OpenShift 叢集的內部登錄。

`ROSAImageRegistryOperatorPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSAImageRegistryOperatorPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 4 月 27 日，UTC 20：13
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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}?",
        "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-${aws:RequestedRegion}?/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ROSAIngressOperatorPolicy

描述：允許 OpenShift 傳入運算子為 Red Hat OpenShift Service on(ROSA) 叢集佈建和管理負載平衡器和網域名稱系統 AWS (DNS) 組態。此政策允許對標籤值的讀取存取權，運算子會篩選 Route 53 資源以探索託管區域。

`ROSAIngressOperatorPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSAIngressOperatorPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 4 月 20 日，UTC 22：37
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ROSAInstallerPolicy

描述：允許 Red Hat OpenShift Service on AWS (ROSA) 安裝程式管理支援 ROSA 叢集安裝 AWS 的資源。這包括管理 ROSA 工作者節點的執行個體描述檔。

`ROSAInstallerPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSAInstallerPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 6 月 6 日 21：00 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

政策版本

政策版本： v10 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "ec2:DescribeCapacityReservations",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEC2",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "GetSecretValue",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ManageRecords",
```

```
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.hypershift.local",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "Route53Manage",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RunInstancesRestrictedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRedHatOwnedAMIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ManageInstancesRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
```

```
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "ListPoliciesAttachedToRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
```

```
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ROSAKMSProviderPolicy

描述：允許內建 ROSA AWS 加密提供者管理 AWS Key Management Service (KMS) 金鑰，以支援使用客戶提供的 AWS KMS 金鑰進行加密的資料加密。此政策允許使用 KMS 金鑰加密和解密資料。

`ROSAKMSProviderPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSAKMSProviderPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 4 月 27 日 20：10 UTC
- 編輯時間：2023 年 4 月 27 日 20：10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ROSAKubeControllerPolicy

描述：允許 ROSA Kubernetes 控制器管理 ROSA 叢集的 Amazon EC2、Elastic Load Balancing (ELB) 和 AWS Key Management Service (KMS) 資源。

`ROSAKubeControllerPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSAKubeControllerPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 4 月 27 日 20：09 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "LoadBalanacerManagement",
      "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" : "LoadBalanacerManagementResourceTag",
      "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ROSAManageSubscription

描述：此政策提供管理 Red Hat OpenShift Service on AWS (ROSA) 訂閱所需的許可。

ROSAManageSubscription 是 AWS 受管政策。

使用此政策

您可以將 ROSAManageSubscription 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2022 年 4 月 11 日 20：58 UTC
- 編輯時間：2023 年 8 月 4 日 19：59 UTC
- ARN: arn:aws:iam::aws:policy/ROSAManageSubscription

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ROSANodePoolManagementPolicy

描述：允許 Red Hat OpenShift Service on AWS (ROSA) 將叢集 EC2 執行個體管理為工作者節點，包括設定安全群組和標記執行個體和磁碟區的許可。此政策也允許使用 EC2 執行個體搭配 AWS Key Management Service (KMS) 金鑰提供的磁碟加密。

`ROSANodePoolManagementPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSANodePoolManagementPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 6 月 8 日 20：48 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

政策版本

政策版本： v8 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "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/*",
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ]
    },
    {
      "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"
```

```
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ROSASharedVPCEndpointPolicy

描述：允許 Red Hat OpenShift Service on AWS (ROSA) 安裝程式設定 VPC 端點和安全群組。預期用於共用 VPC。

`ROSASharedVPCEndpointPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSASharedVPCEndpointPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 11 日 17：19 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCEndpointPolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "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" : "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"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ROSASharedVPCRoute53Policy

描述：允許 Red Hat OpenShift Service on AWS (ROSA) 安裝程式設定 Route53 記錄。預期用於共用 VPC。

ROSASharedVPCRoute53Policy 是 AWS 受管政策。

使用此政策

您可以將 ROSASharedVPCRoute53Policy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 11 日 17：19 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/ROSASharedVPCRoute53Policy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local",
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "ChangeTagsForResourceNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ROSASRESupportPolicy

描述：提供 ROSA 網站可靠性工程 (SRE) 所需的許可，以最初觀察、診斷和支援與 Red Hat OpenShift Service on AWS (ROSA) 叢集相關聯的 AWS 資源，包括變更 ROSA 叢集節點狀態的能力。

ROSASRESupportPolicy 是 AWS 受管政策。

使用此政策

您可以將 ROSASRESupportPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 6 月 1 日 14：36 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DecribeIAMRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeScheduledInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "VPCNetwork",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudtrail",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "DescribeLoadBalancers",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DescribeAddressesAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeAddressesAttribute",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
    },
    {
      "Sid" : "DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeSpotFleetInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSpotFleetInstances",
      "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageInstanceLifecycle",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ROSAWorkerInstancePolicy

描述：允許 Red Hat OpenShift Service on AWS (ROSA) 工作者節點在您帳戶中對 Amazon EC2 執行個體和運算節點生命週期管理 AWS 區域 的唯讀存取。

`ROSAWorkerInstancePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `ROSAWorkerInstancePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2023 年 4 月 20 日、UTC 22：35

- **編輯時間**：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2DescribeInstancesRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRGetAuthorizationToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRReadOnlyAccessRedHatManaged",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
```

```
        "ecr:BatchGetImage",
        "ecr:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

Route53RecoveryReadinessServiceRolePolicy

描述：Route 53 Recovery Readiness 的服務連結角色政策

`Route53RecoveryReadinessServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2021 年 7 月 15 日 16：06 UTC
- 編輯時間：2023 年 2 月 14 日 18：08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

Route53ResolverServiceRolePolicy

描述：允許存取 Route53 Resolver 使用或管理的 AWS 服務 和 資源

Route53ResolverServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 8 月 12 日 17：47 UTC
- 編輯時間：2020 年 8 月 12 日 17：47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

RTBFabricServiceRolePolicy

描述： AWS RTBFabric 建立和管理網路介面資源和交付指標所需的服務連結角色。

RTBFabricServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2025 年 10 月 16 日 16：49 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/RTBFabricServiceRolePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
```

```
      ]
    },
    {
      "Sid" : "RTBFabricRoleCreateTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfacePermissionActions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RTBFabricRolePutMetricDataActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/RTBFabric"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

S3StorageLensServiceRolePolicy

描述：允許存取 AWS 服務 和 S3 Storage Lens 使用或管理的資源

S3StorageLensServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2020 年 11 月 18 日 18：15 UTC
- 編輯時間：2020 年 11 月 18 日 18：15 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioAdminIAMConsolePolicy

描述：透過 和 AWS 管理主控台 SDK 提供 Amazon SageMaker Unified Studio 的初始管理和個別設定權限。允許啟動 SageMaker Unified Studio 入口網站。

`SageMakerStudioAdminIAMConsolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioAdminIAMConsolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 18 日，UTC 22：49
- 編輯時間：2026 年 3 月 5 日 17：42 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMConsolePolicy`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*"
      ]
    },
    {
      "Sid" : "DescribeEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSubnetInTaggedVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroupInVPC",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpointInTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "CreateInternetGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway"
      ],
      "Resource" : "arn:aws:ec2:*:*:internet-gateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedNatGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNatGatewayInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "CreateTaggedRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllocateAddress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ModifyTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AttachInternetGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "Ec2TaggingOperations",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSubnet",
            "CreateSecurityGroup",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateRouteTable",
            "CreateVpcEndpoint"
          ],
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "Ec2TagEIP",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
```

```
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCFNStackCreation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:CreateStack",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteTaggedVpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:DeleteSubnet",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteRouteTable",
        "ec2:DeleteRoute",
        "ec2:ReleaseAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "DeleteTagsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "S3ReadCFNTemplate",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "DataZoneKMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "GlueCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SageMakerStudioAdminIAMDefaultExecutionPolicy

描述：搭配 SageMaker Unified Studio 使用 IAM 角色的管理執行政策。允許管理員佈建、管理和存取您帳戶中的資源（不包括對資料資源的存取），以使用 IAM 為基礎的 SageMaker Unified Studio。

`SageMakerStudioAdminIAMDefaultExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioAdminIAMDefaultExecutionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 18 日 17：19 UTC
- 編輯時間：2026 年 3 月 11 日 17：27 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy`

政策版本

政策版本： v19（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
```

```
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
```

```
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datazone.amazonaws.com",
            "bedrock.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Q",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "ManageSageMakerSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
```

```
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:Batch*",
        "sagemaker:DeleteTags",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:*MlflowApp*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CreateBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
```

```
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFManage",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:connection/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:UseGlueStudio",
```

```
        "glue:*Job*",
        "glue:TestConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBench",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
```

```
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
```

```
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageScheduler",
```

```
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
```

```
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
```

```
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
```

```
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "EMRServerless",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:ListApplications",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:AccessLivyEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SageMakerStudioAdminIAMPermissiveExecutionPolicy

描述：搭配 SageMaker Unified Studio 使用 IAM 角色的管理執行政策。允許管理員佈建、管理和存取本機帳戶中的資源（包括對 S3、Glue、CloudWatch Logs 等資料服務中的所有 APIs 的廣泛存取），以使用 IAM 為基礎的 SageMaker Unified Studio。

`SageMakerStudioAdminIAMPermissiveExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioAdminIAMPermissiveExecutionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 8 月 18 日 17：19 UTC
- 編輯時間：2026 年 3 月 5 日 17：42 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMPermissiveExecutionPolicy`

政策版本

政策版本： v16（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*",
        "s3tables:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "datazone:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
```

```
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "datazone.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
```

```
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
```

```
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnections",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
```

```
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
```

```
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZone*",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
```

```
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioAdminProjectUserRolePolicy

描述：此 IAM 政策會授予 IAM 角色對資料湖操作 AWS Glue Data Catalog （中繼資料） 和 Amazon S3 （實際資料） 的完整存取權，以及依帳戶和角色標籤範圍的存取權。

`SageMakerStudioAdminProjectUserRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioAdminProjectUserRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 7 月 9 日 20：52 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
```

```
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioBedrockAgentServiceRolePolicy

描述：允許 Amazon Bedrock 代理程式存取連接到 SageMaker Studio 中代理程式的 Amazon Bedrock 模型和其他資源。

SageMakerStudioBedrockAgentServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioBedrockAgentServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 2 月 13 日 23：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockAgentServiceRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockApplyGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "LambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrievePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectAttributes"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SageMakerStudioBedrockChatAgentUserRolePolicy

描述：提供存取 Amazon Bedrock 聊天代理程式應用程式的組態和 SageMaker Studio 中的 Amazon Bedrock 代理程式。

`SageMakerStudioBedrockChatAgentUserRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioBedrockChatAgentUserRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 2 月 13 日 23：52 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockChatAgentUserRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "BedrockGetAgentAliasPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetAgentAlias",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGetAndListAgentMetadataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions"
      ],
      "Resource" : "arn:aws:bedrock:*:*:agent/${aws:PrincipalTag/AgentId}",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/AppDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AppDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
```

```
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3ListDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/DataSourcePath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/DataSourcePath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
```

```
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/${aws:PrincipalTag/AgentId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioBedrockEvaluationJobServiceRolePolicy

描述：允許 Amazon Bedrock 存取 SageMaker Studio 中評估任務的 Amazon Bedrock 模型和資料集。

`SageMakerStudioBedrockEvaluationJobServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioBedrockEvaluationJobServiceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 2 月 14 日 00：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockEvaluationJobServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockEvaluationInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelInvocationJob",
        "bedrock:StopModelInvocationJob",
```

```
        "bedrock:GetProvisionedModelThroughput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetBucketLocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketLocation",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
```

```
      "Sid" : "S3EvaluationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/${aws:PrincipalTag/
AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "KmsDescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioBedrockFlowServiceRolePolicy

描述：允許 Amazon Bedrock Flows 存取連接到 SageMaker Studio 中流程的 Amazon Bedrock 模型和其他資源。

SageMakerStudioBedrockFlowServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioBedrockFlowServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 2 月 14 日 00：07 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC

- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFlowServiceRolePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "BedrockGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockApplicationInferenceProfileAccessInProjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "AllowBedrockInvokeModelAccessWithInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/*"
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioBedrockFunctionExecutionRolePolicy

描述：允許 AWS Lambda 在 SageMaker Studio 中存取 Amazon Bedrock 函數元件的組態。

`SageMakerStudioBedrockFunctionExecutionRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioBedrockFunctionExecutionRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 2 月 25 日 03：52 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFunctionExecutionRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "SecretsManagerReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "KMSSameAccountBedrockViaSecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:amazon-bedrock*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

描述：提供在 SageMaker Studio 中設定向量存放區和 Amazon Bedrock 知識庫的存取權。

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 2 月 25 日 03：37 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob"
      ],
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

描述：允許 Amazon Bedrock 知識庫存取 SageMaker Studio 中的 Amazon Bedrock 模型和資料來源。

`SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 2 月 25 日 02：52 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "BedrockModelInvocationPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : [
```

```
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "VectorStoresKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
```

```
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "VectorStoresKmsDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NeptuneGraphDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:GetGraph",
        "neptune-graph:DeleteDataViaQuery",
        "neptune-graph:WriteDataViaQuery",
        "neptune-graph:ReadDataViaQuery"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3VectorsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:GetVectorBucket",
        "s3vectors:GetIndex",
        "s3vectors:PutVectors",
        "s3vectors:GetVectors",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "s3vectors:DeleteVectors"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-${aws:PrincipalTag/
AmazonDataZoneProject}*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:knowledge-base/*"
        }
```

```
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    },
    {
      "Sid" : "SqlWorkbenchAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetSqlRecommendations",
        "sqlworkbench:PutSqlGenerationContext",
        "sqlworkbench:GetSqlGenerationContext",
        "sqlworkbench:DeleteSqlGenerationContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockGenerateQueryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioBedrockPromptUserRolePolicy

描述：提供存取 Amazon Bedrock 提示及其在 SageMaker Studio 中的組態。

SageMakerStudioBedrockPromptUserRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioBedrockPromptUserRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 2 月 14 日 00：22 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockPromptUserRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "BedrockPromptReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/${aws:PrincipalTag/PromptId}:
${aws:PrincipalTag/PromptVersion}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/PromptDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/PromptDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/${aws:PrincipalTag/PromptId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
```

```
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioDomainExecutionRolePolicy

描述：Amazon SageMaker Studio 使用此政策來編目、探索、管理、共用和分析 Amazon SageMaker Studio 網域中的資料。

`SageMakerStudioDomainExecutionRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioDomainExecutionRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2024 年 11 月 20 日 21：56 UTC
- 編輯時間：2026 年 2 月 26 日 00：42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainExecutionRolePolicy`

政策版本

政策版本： v20 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:AssociateGovernedTerms",
        "datazone:BatchGetAttributesMetadata",
        "datazone:BatchPutAttributesMetadata",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateConnection",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
```

```
            "datazone:DeleteAssetType",
            "datazone:DeleteConnection",
            "datazone:DeleteDataProduct",
            "datazone:DeleteDataSource",
            "datazone:DeleteDomainUnit",
            "datazone:DeleteEnvironment",
            "datazone:DeleteEnvironmentProfile",
            "datazone:DeleteFormType",
            "datazone:DeleteGlossary",
            "datazone:DeleteGlossaryTerm",
            "datazone:DeleteListing",
            "datazone:DeleteProject",
            "datazone:DeleteProjectMembership",
            "datazone:DeleteRule",
            "datazone:DeleteSubscriptionGrant",
            "datazone:DeleteSubscriptionRequest",
            "datazone:DeleteSubscriptionTarget",
            "datazone:DeleteTimeSeriesDataPoints",
            "datazone:DisassociateGovernedTerms",
            "datazone:GetAsset",
            "datazone:GetAssetFilter",
            "datazone:GetAssetType",
            "datazone:GetConnection",
            "datazone:GetDataProduct",
            "datazone:GetDataSource",
            "datazone:GetDataSourceRun",
            "datazone:GetDomain",
            "datazone:GetDomainUnit",
            "datazone:GetEnvironment",
            "datazone:GetEnvironmentAction",
            "datazone:GetEnvironmentActionLink",
            "datazone:GetEnvironmentBlueprint",
            "datazone:GetEnvironmentBlueprintConfiguration",
            "datazone:GetEnvironmentCredentials",
            "datazone:GetEnvironmentProfile",
            "datazone:GetFormType",
            "datazone:GetGlossary",
            "datazone:GetGlossaryTerm",
            "datazone:GetGroupProfile",
            "datazone:GetLineageNode",
            "datazone:GetListing",
            "datazone:GetMetadataGenerationRun",
            "datazone:GetProject",
            "datazone:GetRule",
```

```
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUpdateEligibility",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListConnections",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:QueryGraph",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
```

```
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "q:GetIdentityMetadata",
        "glue:StartCompletion",
```

```
        "glue:GetCompletion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q/${aws:PrincipalTag/datazone-
domainId}*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/${aws:PrincipalTag/datazone-
domainId}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
```

```
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ListCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "UseCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ProjectProfilePermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetProjectProfile",
        "datazone:ListProjectProfiles"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    },
    {
      "Sid" : "AccountPoolPermissionsStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetAccountPool",
        "datazone:ListAccountPools",
        "datazone:ListAccountsInAccountPool"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioDomainServiceRolePolicy

描述：Amazon SageMaker Studio 在入口網站中執行的網域層級動作的服務角色。

SageMakerStudioDomainServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioDomainServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2024 年 11 月 20 日 21：56 UTC
- 編輯時間：2024 年 11 月 20 日 21：56 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles/*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com",
          "kms:EncryptionContext:PARAMETER_ARN" : "arn:aws:ssm:*:*:parameter/amazon/
datazone/profiles*"
        }
      }
    }
```

```
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioEMRContainersSystemNamespaceRolePolicy

描述：Amazon SageMaker Studio 會為專案使用者建立 IAM 角色，以執行資料分析、人工智慧和機器學習動作，並在建立這些角色時使用此政策來定義與 EMR 相關的許可。

`SageMakerStudioEMRContainersSystemNamespaceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioEMRContainersSystemNamespaceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 10 月 23 日 18：34 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRContainersSystemNamespaceRolePolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AssumeProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "TagSessionProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/LakeFormationAuthorizedCaller" : "EMR on EKS Engine",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "SetContextProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SageMakerStudioEMRInstanceRolePolicy

描述：Amazon SageMaker Studio 會為專案使用者建立 IAM 角色，以執行資料分析、人工智慧和機器學習動作，並在建立這些角色時使用此政策來定義與 EMR 相關的許可。

`SageMakerStudioEMRInstanceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioEMRInstanceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 2 月 27 日 00：22 UTC
- 編輯時間：2026 年 2 月 12 日 17：57 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRInstanceRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCertificateLocationS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AccessPatchingRPMsS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessBootstrapActionScriptS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/bootstrap-script/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EMRClusterLogUploadS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRRuntimeRoleAssumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "iam:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SageMakerStudioEMRServiceRolePolicy

描述：Amazon SageMaker Studio 會為專案使用者建立 IAM 角色，以執行資料分析、人工智慧和機器學習動作，並在建立這些角色時使用此政策來定義與 EMR 相關的許可。

SageMakerStudioEMRServiceRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioEMRServiceRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 1 月 31 日 19：52 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassRoleToEMREC2InstanceRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_
${aws:PrincipalTag/AmazonDataZoneProject}_${aws:PrincipalTag/
AmazonDataZoneEnvironment}",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneEnvironment" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateInNetworkForSharedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
```

```
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeKeyForLogPusherCMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioFullAccess

描述：此政策透過 Amazon SageMaker 管理主控台提供 Amazon SageMaker Unified Studio 的完整存取權。

SageMakerStudioFullAccess 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioFullAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 28 日 00：06 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioFullAccess

政策版本

政策版本： v15 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "iam:ListPolicies",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies",
        "quicksight:DescribeAccountSubscription",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
```

```
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "ReadManagedBlueprintTemplatesStatement",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PutObjectStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
```

```
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
```

```
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "ModelAccessUseCaseStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:PutUseCaseForModelAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioProjectProvisioningRolePolicy

描述：Amazon SageMaker Studio 使用此政策來佈建和管理您帳戶中的資源。

SageMakerStudioProjectProvisioningRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioProjectProvisioningRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2024 年 11 月 20 日 21：58 UTC
- 編輯時間：2026 年 3 月 11 日 16：27 UTC
- ARN: arn:aws:iam::aws:policy/service-role/SageMakerStudioProjectProvisioningRolePolicy

政策版本

政策版本： v78 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CfnMng",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CfnDelete",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "bedrock:ListEvaluationJobs",
        "cloudformation:ValidateTemplate",
        "codecommit:ListRepositories",
        "eks:DescribeCluster",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "glue:DescribeConnectionType",
        "glue:ListConnectionTypes",
        "glue:*GlueIdentityCenterConfiguration",
        "iam:ListPolicies",
        "logs:DescribeLogGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeDataShares",
        "redshift:DescribeDataSharesForConsumer",
        "redshift:GetResourcePolicy",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFMng",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
```

```
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:DescribeResource",
        "lakeformation:*LakeFormationIdentityCenterConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DzTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DzCfTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::amazon-sagemaker-cf-templates*/*"
    },
    {
      "Sid" : "CcCreate",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateRepository",
        "codecommit:TagResource"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CcDelete",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:DeleteRepository",
        "codecommit:UntagResource",
        "codecommit:UpdateRepositoryEncryptionKey",
        "codecommit:PutRepositoryTriggers"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CcAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetBranch",
        "codecommit:CreateCommit",
        "codecommit:GetRepository",
        "codecommit:GetFile"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "CcKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        }
      }
    },
    {
      "Sid" : "GetIamRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ]
    },
    {
      "Sid" : "IAMMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
```

```
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrockExecution*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/AmazonBedrockConsumptionRole*",
        "arn:aws:iam::*:role/AmazonBedrockEvaluation*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamDzMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RoleCreate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRContainersSystemNamespaceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRInstanceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole",
            "arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "IamMngAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneAdminProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "IamMngBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockAgentServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockChatAgentUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFlowServiceRolePolicy",
```

```
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFunctionExecutionRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockPromptUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockEvaluationJobServiceRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "IamTag",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/datazone_redshift_serverless_admin_role_*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "BootstrappedServices",
            "AmazonBedrockManaged",
            "RedshiftDb*",
            "EnableAmazonBedrockPermissions",
            "EnableAmazonBedrockIDEPermissions",
            "EnableGlueWorkloadsPermissions",
```

```
            "EnableSageMakerMLWorkloadsPermissions",
            "DomainBucketName",
            "KmsKeyId",
            "DomainKmsKeyId",
            "DefaultGlueCatalogKmsKeyId",
            "LogGroupName",
            "RoleName",
            "vpcArn",
            "VpcId",
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
    {
      "Sid" : "AdminProjectTagRoleMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneScopeName",
            "BootstrappedServices",
            "AmazonDataZoneAdminProject"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "DomainBucketName",
            "KmsKeyId",
            "AgentId",
            "AgentAliasId",
            "AppDefinitionPath",
            "DataSourcePath",
            "PromptId",
            "PromptVersion",
            "PromptDefinitionPath",
            "OpenSearchServerlessCollectionId"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagRS",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "RedshiftDb*"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "IamTagEMR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*",
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*",
        "arn:aws:iam::*:role/datazone_emr_containers_system_namespace_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "DataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "DomainBucketName",
            "KmsKeyId",
            "VpcId"
          ]
        }
      }
    },
    {
      "Sid" : "IamUntag",
      "Effect" : "Allow",
      "Action" : "iam:UntagRole",
      "Resource" : "arn:aws:iam::*:role/datazone_usr_role_*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "EnableAmazonBedrockIDEPermissions"
        }
      }
    },
    {
      "Sid" : "MngRoles",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DzMngRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateAssumeRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_emr_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamAttach",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "IamDetach",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ]
    },
    {
      "Sid" : "DzMngPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:CreatePolicyVersion",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:iam::*:policy/connector-manage-access-policy*",
        "arn:aws:iam::*:policy/SageMakerStudioQueryExecutionRolePolicy"
      ]
    },
    {
      "Sid" : "InstanceProfile",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ],
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow.amazonaws.com",
            "athena.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForDZ",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForGlue",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmr",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticmapreduce.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "PassRoleForEmrIP",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBR",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRoleToLambda",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AossSLR",
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog/*",
        "arn:aws:glue:*:*:database/s3tablescatalog/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnGlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "GlueDbTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbDelete",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
```

```
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "GlueConnTag",
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnMng",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnections",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnections",
        "glue:GetTags"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Effect" : "Allow",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaConnection",
      "Action" : [
        "athena:CreateDataCatalog"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "ConnectionTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "federated_athena*"
          ]
        }
      }
    },
    {
      "Sid" : "CreateConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngCatalogConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "GetDataCatalogEncSett",
      "Action" : "glue:GetDataCatalogEncryptionSettings",
      "Effect" : "Allow",
      "Resource" : "arn:aws:glue:*:*:catalog",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Repo",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:GetCloudFormationTemplate",
        "serverlessrepo:CreateCloudFormationTemplate"
      ],
      "Resource" : [
        "arn:aws:serverlessrepo:*:*:applications/Athena*"
      ]
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/athena-federation-repository*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CfnChangeSet",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:transform/Serverless*"
      ]
    },
    {
      "Sid" : "LambdaMng",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "LambdaGet",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : [
            "athena.amazonaws.com",
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "TagLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*",
            "federated_athena*",
            "lambda:createdBy"
          ]
        }
      }
    },
    {
      "Sid" : "LambdaS3Get",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaLast" : [
            "lambda.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "s3:prefix" : "true"
        }
      }
    },
    {
      "Sid" : "S3Create",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "Cfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
```

```
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/athenafederatedcatalog*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/federated_athena_datacatalog" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaDC",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteDataCatalog",
        "athena:GetDataCatalog",
        "athena:UpdateDataCatalog"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Action" : [
```

```
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "S3tPassConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/aws:s3tables"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCatalogCreate",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCatalog"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GlueCatalogMgmt",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RSMng",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteNamespace",
        "redshift-serverless:DeleteWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:GetNamespace",
```

```
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshotcopyconfiguration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataShare",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AssociateDataShareConsumer",
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "redshift-serverless.amazonaws.com",
            "glue.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
```

```
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
```

```
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SGMng",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGRevoke",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagEc2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "EC2Mng",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CreateLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged"
          ]
        }
      }
    },
    {
      "Sid" : "LGRetention",
      "Effect" : "Allow",
      "Action" : "logs:PutRetentionPolicy",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngLG",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:UntagResource",
        "logs:DeleteRetentionPolicy",
        "logs:GetDataProtectionPolicy",
        "logs:PutDataProtectionPolicy",
        "logs:DeleteDataProtectionPolicy",
        "logs:AssociateKmsKey",
        "logs:DisassociateKmsKey",
        "logs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaMng",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AthenaWGDelete",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "athena:UpdateWorkGroup",
        "athena:UntagResource",
        "athena:GetWorkGroup"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftCreate",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "TagRSS",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MngSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false"
        }
      }
    },
    {
      "Sid" : "SecretProject",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SecretAll",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "TagSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "CreatedBy"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "SecretKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SsoKms",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IdStoreKms",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
```

```
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/emr-containers.amazonaws.com/
AWSServiceRoleForAmazonEMRContainers",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "RssMng",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:UntagResource",
        "redshift-serverless:UpdateNamespace",
        "redshift-serverless:UpdateWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "redshift-serverless.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:redshift-serverless:arn" : "false"
        }
      }
    },
    {
      "Sid" : "BRSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:TagResource"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRsSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "Redshift",
            "aws:secretsmanager:*",
            "aws:redshift-serverless:*",
            "AmazonDataZone*",
```

```
            "datazone.rs.workgroup"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagSMDForUpdate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain",
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
        "arn:aws:sagemaker:*:*:mlflow-app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateDomain",
        "sagemaker:DeleteDomain"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SMAppDelete",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteApp",
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSpace",
      "Effect" : "Allow",
```

```
      "Action" : "sagemaker:DeleteSpace",
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteUserProfile",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteUserProfile",
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrSCreate",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:CreateApplication",
        "emr-serverless:TagResource"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
```

```
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "EmrSMng",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:DeleteApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:UpdateApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Eni",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Subnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MLFlowCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowTrackingServer",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MLFlowDescribe",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeMlflowTrackingServer",
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
    },
    {
      "Sid" : "MLFlowDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowTrackingServer"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MLFlowServerlessCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MLFlowServerlessDescribeDelete",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteMlflowApp",
        "sagemaker:DescribeMlflowApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AossMng",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:UpdateAccessPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*",
```

```
          "aoss:index" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "MngAossPolicies",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetAoss",
      "Effect" : "Allow",
      "Action" : "aoss:BatchGetCollection",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AossCollections",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection",
        "aoss:UpdateCollection",
        "aoss:DeleteCollection",
        "aoss:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:UpdateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:GetGraph"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3VectorsMng",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:CreateVectorBucket",
        "s3vectors:DeleteVectorBucket",
        "s3vectors:ListVectorBuckets",
        "s3vectors:GetVectorBucket",
        "s3vectors:CreateIndex",
        "s3vectors:DeleteIndex",
        "s3vectors:ListIndexes",
        "s3vectors:GetIndex"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "TagNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:TagResource"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrock*"
          ]
        }
      }
    },
    {
      "Sid" : "GetS3GenAI",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/dzd*/*/genAI/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetBR",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetGuardrail",
        "bedrock:GetPrompt",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:ListTagsForResource"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BRMng",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateAgent",
        "bedrock:UpdateAgent",
        "bedrock:PrepareAgent",
        "bedrock:DeleteAgent",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentAlias",
        "bedrock:CreateAgentAlias",
        "bedrock:UpdateAgentAlias",
        "bedrock:DeleteAgentAlias",
        "bedrock:ListAgentActionGroups",
        "bedrock:GetAgentActionGroup",
        "bedrock:CreateAgentActionGroup",
        "bedrock:UpdateAgentActionGroup",
        "bedrock:DeleteAgentActionGroup",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:AssociateAgentKnowledgeBase",
        "bedrock:DisassociateAgentKnowledgeBase",
        "bedrock:UpdateAgentKnowledgeBase",
        "bedrock:CreateKnowledgeBase",
        "bedrock:UpdateKnowledgeBase",
        "bedrock:DeleteKnowledgeBase",
        "bedrock:ListDataSources",
        "bedrock:GetDataSource",
        "bedrock:CreateDataSource",
        "bedrock:UpdateDataSource",
        "bedrock:DeleteDataSource",
        "bedrock:ListIngestionJobs",
        "bedrock:GetIngestionJob",
        "bedrock:StartIngestionJob",
        "bedrock:StopIngestionJob",
        "bedrock:CreateGuardrail",
        "bedrock:UpdateGuardrail",
```

```
        "bedrock:DeleteGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreatePrompt",
        "bedrock:UpdatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:CreateFlow",
        "bedrock:UpdateFlow",
        "bedrock:PrepareFlow",
        "bedrock:DeleteFlow",
        "bedrock:ListFlowAliases",
        "bedrock:GetFlowAlias",
        "bedrock:CreateFlowAlias",
        "bedrock:UpdateFlowAlias",
        "bedrock:DeleteFlowAlias",
        "bedrock:ListFlowVersions",
        "bedrock:GetFlowVersion",
        "bedrock:CreateFlowVersion",
        "bedrock:DeleteFlowVersion",
        "bedrock:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagBR",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : [
        "arn:aws:bedrock:*:*:agent-alias/*/TSTALIASID",
        "arn:aws:bedrock:*:*:flow/*/alias/TSTALIASID"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
```

```
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:BatchDeleteEvaluationJob",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "BRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:GetPolicy",
        "lambda:AddPermission",
        "lambda:TagResource"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "MngBRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRClusterMng",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowEnv",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:DeleteEnvironment",
        "airflow:TagResource"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpcCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ENICreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "KmsCreate",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "airflow.*.amazonaws.com",
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "KmsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QueryRoleMng",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
```

```
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "QueryRoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "QueryRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioQueryExecutionRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "TagQueryRole",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
```

```
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
    {
      "Sid" : "ListQueryPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "EMRCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrRoleCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone_emr_*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "EmrInstanceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListTagsForResource",
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ScheduleGroup",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteScheduleGroup",
        "scheduler:UntagResource"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "CreateSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:CreateScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        }
      }
    },
    {
      "Sid" : "TagSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:TagResource",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        }
      }
    },
    {
      "Sid" : "DeleteSchedule",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/SageMakerUnifiedStudio-*-*/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngQSFolder",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:CreateFolder",
        "quicksight:CreateFolderMembership",
        "quicksight:CreateVPCConnection",
        "quicksight:DeleteDataSource",
        "quicksight:DeleteFolder",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListFolderMembers",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:UpdateFolder",
        "quicksight:UpdateFolderPermissions",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "QuickSightResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeGroup",
        "quicksight:DescribeGroupMembership",
        "quicksight:DescribeUser",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDashboardPermissions"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagQS",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:TagResource"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "PassRoleForQS",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQuickSightVPC",
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "quicksight.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.quicksight",
            "aws.codecommit"
          ]
        },
        "Null" : {
          "events:source" : "false",
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "datazone.amazonaws.com",
          "events:detail-type" : [
            "AWS Service Event via CloudTrail",
            "CodeCommit Repository State Change"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "MngEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "datazone.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RssAdmin",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3AGPerm",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstance",
        "s3:CreateAccessGrantsInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "ResourceTagsUnTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:UntagResource",
        "neptune-graph:UntagResource",
        "quicksight:UntagResource",
        "glue:UntagResource",
        "airflow:UntagResource",
        "secretsmanager:UntagResource",
        "lambda:UntagResource",
        "emr-serverless:UntagResource",
        "elasticmapreduce:RemoveTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SSOMng",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "elasticmapreduce.amazonaws.com",
            "emr-containers.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "ops.emr-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EmrContainersMng",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:CreateManagedEndpoint",
        "emr-containers:CreateSecurityConfiguration",
        "emr-containers:CreateVirtualCluster",
        "emr-containers:DeleteManagedEndpoint",
        "emr-containers:DeleteSecurityConfiguration",
        "emr-containers:DeleteVirtualCluster",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MngViaEmrContainers",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:RevokeSecurityGroupIngress",
        "eks:AssociateAccessPolicy",
        "eks:CreateAccessEntry",
        "eks:DisassociateAccessPolicy",
        "eks:DeleteAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioProjectRoleMachineLearningPolicy

描述：Amazon SageMaker Studio 會為專案使用者建立 IAM 角色，以執行資料分析、人工智慧和機器學習動作，並在建立這些角色時使用此政策來定義與 SageMaker 相關的許可。

`SageMakerStudioProjectRoleMachineLearningPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioProjectRoleMachineLearningPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 20 日 21：55 UTC
- 編輯時間：2026 年 2 月 26 日 21：42 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy`

政策版本

政策版本： v38 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowManageSageMakerEniOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "sagemaker.amazonaws.com",
            "airflow.amazonaws.com"
          ]
        },
        "ArnLike" : {
```

```
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerTrainingEniOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "AllowSageMakerCreateVpcEndpointOnVpcId",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}",
      "Condition" : {
        "StringEquals" : {
          "ec2:VpcID" : "${aws:PrincipalTag/VpcId}"
        },
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDescribeVPCResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeDhcpOptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSageMakerLogAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "SageMakerMlflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerMlflowServerlessPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowApp",
        "sagemaker:CreatePresignedMlflowAppUrl",
        "sagemaker:DeleteMlflowApp",
        "sagemaker:DescribeMlflowApp",
        "sagemaker:UpdateMlflowApp",
        "sagemaker:CallMlflowAppApi"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-app/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerBYOFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerBYOIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeImageVersion",
        "sagemaker:ListImageVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeImageActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeImage"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:image/*"
    },
    {
      "Sid" : "SageMakerPipelinesSTSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerLogPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "SageMakerCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateInferenceRecommendationsJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerInferencePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
```

```
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerUpdateInferenceComponentRuntimeConfigAutoscalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateInferenceComponentRuntimeConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "SageMakerDescribeUpdateDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:UpdatePipeline",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DeletePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopPipelineExecution",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:AddAssociation",
        "sagemaker:DeleteAssociation",
```

```
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteArtifact"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerModelRegistryLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:QueryLineage",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:GetSearchSuggestions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
```

```
        "sagemaker:ListHubs",
        "sagemaker:ListPipelines",
        "sagemaker:ListContexts",
        "sagemaker:ListMlflowApps"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerSearchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Search"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "sagemaker:SearchVisibilityCondition/Tags.AmazonDataZoneProject/
EqualsIfExists" : "${aws:PrincipalTag/AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerListPermissionsTagRestricted",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubContents",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
```

```
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "SageMakerECRGetAuthorizationTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerMLFlowModelRegistrationPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:model-package-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForTaggedUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "SageMakerStudioAppListActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListSpaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeDomainActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeJupyterLabAppActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ]
    },
    {
      "Sid" : "SageMakerStudioAppDescribeUserProfileActionPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeTaggedUserProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SMStudioAppDescribeSpaceActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeSpace"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingTaggedOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        },
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
```

```
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        },
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
```

```
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PublishSagemakerMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "/aws/sagemaker/*"
        }
      }
    },
    {
      "Sid" : "ManageSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MutateSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
    },
    {
      "Sid" : "SageMakerJumpstartS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-*/*"
      ],
```

```
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCrossAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:ListModelPackages",
        "sagemaker:CreateModel"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerListTagsRestrictionOnSharedResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissionsWithserviceNamespace",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeregisterScalableTarget",
```

```
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "application-autoscaling:service-namespace" : "sagemaker"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "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" : "SageMakerKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGObjectRead",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        }
      }
    },
    {
      "Sid" : "S3AGObjectWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
```

```
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        }
      }
    },
    {
      "Sid" : "S3AGBucketLevelReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        }
      }
    },
    {
      "Sid" : "S3AGKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        }
      }
    },
    {
      "Sid" : "S3AGLocationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrantsLocation",
        "s3:DeleteAccessGrantsLocation",
        "s3:GetAccessGrantsLocation"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:accessGrantsLocationScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/"
        }
      }
    },
    {
      "Sid" : "S3AGPermissionManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrant",
        "s3:DeleteAccessGrant"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
```

```
        "StringLike" : {
          "s3:accessGrantScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "s3:AccessGrants"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutAccessGrantsInstanceResourcePolicy"
      ],
      "Resource" : "arn:aws:s3:*:*:access-grants/default",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:TagResource",
        "s3:ListTagsForResource"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsumerS3AGPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MLAccountDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:ListWorkflow*",
        "airflow-serverless:ListTask*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowServerlessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:GetTaskInstance",
        "airflow-serverless:GetWorkflow",
        "airflow-serverless:GetWorkflowRun",
        "airflow-serverless:ListTagsForResource",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource",
```

```
        "airflow-serverless:UpdateWorkflow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/mwaa-serverless/${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ]
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
```

```
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless"
      ]
    },
    {
      "Sid" : "DataZoneUserPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GenerateCode",
        "datazone:SendMessage",
        "datazone:*Conversation*",
        "datazone:*Cell*",
        "datazone:*Notebook*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AthenaSession",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard",
        "athena:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBenchMLActionsWithResourceType",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioProjectUserRolePermissionsBoundary

描述：Amazon SageMaker 為 Projects 使用者建立 IAM 角色，以執行資料分析、人工智慧和機器學習動作，並在建立這些角色時使用此政策來定義其許可界限。

SageMakerStudioProjectUserRolePermissionsBoundary 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioProjectUserRolePermissionsBoundary 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 20 日 21：57 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePermissionsBoundary

政策版本

政策版本： v19 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAllNonMatchingProjectTag",
      "Effect" : "Deny",
      "Action" : "*",
      "NotResource" : [
        "arn:*:sagemaker:*:*:model-package-group/*",
        "arn:*:sagemaker:*:*:model-package/*",
        "arn:*:glue:*:*:catalog/*",
```

```
        "arn:*:glue:*:*:database/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
```

```
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEmrEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "codecommit.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
```

```
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSManagementPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants",
        "kms:GetPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "DataZoneDescribeKMSPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
```

```
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaFederatedCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
"arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
```

```
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessCertificateS3LocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
```

```
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchDescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:StartQuery",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/*",
```

```
        "arn:aws:logs:*:*:log-group:airflow*",
        "arn:aws:logs:*:*:log-group:datazone*"
      ]
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
```

```
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
```

```
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
```

```
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCrawlerPermissions",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UseGlueStudio",
        "glue:ListSessions",
        "glue:StartCompletion",
        "glue:GetCompletion",
        "glue:GetGeneratedCode",
        "glue:GetTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GluePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:CancelStatement",
        "glue:ListStatements",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:StopSession",
```

```
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:DeleteDataQualityRuleset",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:UpdateDataQualityRuleset"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "ec2.amazonaws.com",
            "emr-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:PassAccountSettings",
```

```
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQSqlPromptQuotas",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAccessExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RedshifServerlessCredentialsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "redshift-data.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "GenerativeAIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:*-model/*"
```

```
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "ManageNetworkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListImageVersions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListInferenceComponents",
```

```
            "sagemaker:ListEndpoints",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListModels",
            "sagemaker:ListModelPackages",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelMetadata",
            "sagemaker:ListMlflowTrackingServers",
            "sagemaker:ListArtifacts",
            "sagemaker:ListAssociations",
            "sagemaker:ListHubContents",
            "sagemaker:ListHubs",
            "sagemaker:ListPipelineExecutionSteps",
            "sagemaker:ListPipelineExecutions",
            "sagemaker:ListPipelineParametersForExecution",
            "sagemaker:ListPipelines",
            "sagemaker:ListApps",
            "sagemaker:ListDomains",
            "sagemaker:ListUserProfiles",
            "sagemaker:ListSpaces",
            "sagemaker:ListTags",
            "sagemaker:DescribeMlflowTrackingServer",
            "sagemaker:DescribeImageVersion",
            "sagemaker:DescribeImage",
            "sagemaker:DescribeInferenceComponent",
            "sagemaker:DescribeEndpointConfig",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeOptimizationJob",
            "sagemaker:DescribeEndpoint",
            "sagemaker:DescribeInferenceRecommendationsJob",
            "sagemaker:DescribeModelPackage",
            "sagemaker:DescribeModelPackageGroup",
            "sagemaker:DescribePipeline",
            "sagemaker:DescribePipelineExecution",
            "sagemaker:DescribePipelineDefinitionForExecution",
            "sagemaker:DescribeHyperParameterTuningJob",
            "sagemaker:DescribeAutoMLJob",
            "sagemaker:DescribeAutoMLJobV2",
            "sagemaker:DescribeProcessingJob",
            "sagemaker:DescribeTrainingJob",
            "sagemaker:DescribeAction",
            "sagemaker:DescribeArtifact",
            "sagemaker:DescribeTrialComponent",
            "sagemaker:DescribeContext",
            "sagemaker:DescribeDomain",
```

```
            "sagemaker:DescribeApp",
            "sagemaker:DescribeUserProfile",
            "sagemaker:DescribeSpace",
            "sagemaker:AddTags",
            "sagemaker:AddAssociation",
            "sagemaker:DeleteAssociation",
            "sagemaker:DeleteContext",
            "sagemaker:DeleteAction",
            "sagemaker:DeleteArtifact",
            "sagemaker:DeleteUserProfile",
            "sagemaker:UpdateSpace",
            "sagemaker:DeleteSpace",
            "sagemaker:DeleteApp",
            "sagemaker:CreatePresignedDomainUrl",
            "sagemaker:CreateUserProfile",
            "sagemaker:CreateSpace",
            "sagemaker:CreateApp",
            "sagemaker:CreateTrainingJob",
            "sagemaker:CreateTransformJob",
            "sagemaker:CreateProcessingJob",
            "sagemaker:CreateAutoMLJob",
            "sagemaker:CreateAutoMLJobV2",
            "sagemaker:CreateHyperParameterTuningJob",
            "sagemaker:CreateEndpointConfig",
            "sagemaker:CreateEndpoint",
            "sagemaker:CreateModel",
            "sagemaker:CreateModelPackage",
            "sagemaker:CreateModelPackageGroup",
            "sagemaker:CreatePipeline",
            "sagemaker:CreateContext",
            "sagemaker:CreateArtifact",
            "sagemaker:CreateAction",
            "sagemaker:CreateInferenceComponent",
            "sagemaker:UpdateInferenceComponentRuntimeConfig",
            "sagemaker:StopTrainingJob",
            "sagemaker:StopProcessingJob",
            "sagemaker:StopAutoMLJob",
            "sagemaker:StopHyperParameterTuningJob",
            "sagemaker:DescribeTransformJob",
            "sagemaker:StopTransformJob",
            "sagemaker:UpdateTrainingJob",
            "sagemaker:BatchGetMetrics",
            "sagemaker:BatchPutMetrics",
            "sagemaker:DeleteEndpointConfig",
```

```
            "sagemaker:DeleteEndpoint",
            "sagemaker:UpdateEndpoint",
            "sagemaker:UpdateEndpointWeightsAndCapacities",
            "sagemaker:BatchDescribeModelPackage",
            "sagemaker:UpdateModelPackage",
            "sagemaker:DeleteModel",
            "sagemaker:DeleteModelPackage",
            "sagemaker:DeleteModelPackageGroup",
            "sagemaker:DeleteTags",
            "sagemaker:DeleteInferenceComponent",
            "sagemaker:CreateInferenceRecommendationsJob",
            "sagemaker:InvokeEndpoint",
            "sagemaker:InvokeEndpointAsync",
            "sagemaker:InvokeEndpointWithResponseStream",
            "sagemaker:QueryLineage",
            "sagemaker:UpdatePipeline",
            "sagemaker:DeletePipeline",
            "sagemaker:UpdatePipelineExecution",
            "sagemaker:StartPipelineExecution",
            "sagemaker:StopPipelineExecution",
            "sagemaker:RetryPipelineExecution",
            "sagemaker:SendPipelineExecutionStepSuccess",
            "sagemaker:SendPipelineExecutionStepFailure",
            "sagemaker:GetSearchSuggestions",
            "sagemaker:Search",
            "sagemaker:UpdateMlflowTrackingServer",
            "sagemaker:StartMlflowTrackingServer",
            "sagemaker:StopMlflowTrackingServer",
            "sagemaker:CreatePresignedMlflowTrackingServerUrl",
            "sagemaker:ListPartnerApps",
            "sagemaker:CreatePartnerAppPresignedUrl",
            "sagemaker:DescribePartnerApp",
            "sagemaker:CallPartnerAppApi",
            "sagemaker-mlflow:AccessUI",
            "sagemaker-mlflow:CreateExperiment",
            "sagemaker-mlflow:SearchExperiments",
            "sagemaker-mlflow:GetExperiment",
            "sagemaker-mlflow:GetExperimentByName",
            "sagemaker-mlflow:DeleteExperiment",
            "sagemaker-mlflow:RestoreExperiment",
            "sagemaker-mlflow:UpdateExperiment",
            "sagemaker-mlflow:CreateRun",
            "sagemaker-mlflow:DeleteRun",
            "sagemaker-mlflow:RestoreRun",
```

```
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:LogMetric",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:LogModel",
        "sagemaker-mlflow:LogInputs",
        "sagemaker-mlflow:SetExperimentTag",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:DeleteTag",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker-mlflow:CreateRegisteredModel",
        "sagemaker-mlflow:GetRegisteredModel",
        "sagemaker-mlflow:RenameRegisteredModel",
        "sagemaker-mlflow:UpdateRegisteredModel",
        "sagemaker-mlflow:DeleteRegisteredModel",
        "sagemaker-mlflow:GetLatestModelVersions",
        "sagemaker-mlflow:CreateModelVersion",
        "sagemaker-mlflow:GetModelVersion",
        "sagemaker-mlflow:UpdateModelVersion",
        "sagemaker-mlflow:DeleteModelVersion",
        "sagemaker-mlflow:SearchModelVersions",
        "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
        "sagemaker-mlflow:TransitionModelVersionStage",
        "sagemaker-mlflow:SearchRegisteredModels",
        "sagemaker-mlflow:SetRegisteredModelTag",
        "sagemaker-mlflow:DeleteRegisteredModelTag",
        "sagemaker-mlflow:DeleteModelVersionTag",
        "sagemaker-mlflow:DeleteRegisteredModelAlias",
        "sagemaker-mlflow:SetRegisteredModelAlias",
        "sagemaker-mlflow:GetModelVersionByAlias",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:DescribeImages",
        "elasticfilesystem:DescribeMountTargets",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "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" : "ComputePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "sts:GetCallerIdentity",
        "sts:TagSession",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
```

```
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:TerminateJobFlows",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataLakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
```

```
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
```

```
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EMRServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeletePlacementGroup",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
```

```
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupMutatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        }
      }
    },
    {
      "Sid" : "ModelRegistryBedRockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AccessAossCollectionsForBedrock",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:InvokeAgent",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateEvaluationJobForFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseDataIngestionKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "kms:ViaService" : "true",
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetDataZoneEnvironmentCfnStackPermissionsForBedrockAppExport",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "MWAAPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments",
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
    },
    {
      "Sid" : "SQSPermissionsForMWAA",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : "arn:aws:sqs:*:*:airflow-celery-*"
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueConnectionAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretAccessForForUseWithAllDataZoneProjectsSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "AccessForDynamoDbConnections",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForAthenaCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-staging-bucket-*/*",
        "arn:aws:s3:::redshift-staging-bucket-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "GetS3ObjectForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*/dzd_*/*/dev/sys/athena/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "airflow:CreateWebLoginToken",
        "airflow:GetEnvironment",
        "airflow:InvokeRestApi",
        "airflow:ListEnvironments",
        "airflow:UpdateEnvironment",
        "aoss:APIAccessAll",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
```

```
            "athena:GetQueryExecution",
            "athena:GetQueryResults",
            "athena:GetQueryResultsStream",
            "athena:GetQueryRuntimeStatistics",
            "athena:GetSession",
            "athena:GetSessionStatus",
            "athena:GetTableMetadata",
            "athena:GetWorkGroup",
            "athena:ImportNotebook",
            "athena:ListDatabases",
            "athena:ListDataCatalogs",
            "athena:ListEngineVersions",
            "athena:ListNamedQueries",
            "athena:ListPreparedStatements",
            "athena:ListQueryExecutions",
            "athena:ListTableMetadata",
            "athena:ListTagsForResource",
            "athena:ListWorkGroups",
            "athena:StartCalculationExecution",
            "athena:StartQueryExecution",
            "athena:StartSession",
            "athena:StopCalculationExecution",
            "athena:StopQueryExecution",
            "athena:TerminateSession",
            "athena:UpdateNamedQuery",
            "athena:UpdateNotebook",
            "athena:UpdateNotebookMetadata",
            "athena:UpdatePreparedStatement",
            "bedrock:ApplyGuardrail",
            "bedrock:BatchDeleteEvaluationJob",
            "bedrock:CreateAgentAlias",
            "bedrock:CreateEvaluationJob",
            "bedrock:CreatePrompt",
            "bedrock:CreatePromptVersion",
            "bedrock:DeleteAgentAlias",
            "bedrock:DeleteAgentVersion",
            "bedrock:DeletePrompt",
            "bedrock:GetAgent",
            "bedrock:GetAgentActionGroup",
            "bedrock:GetAgentAlias",
            "bedrock:GetAgentKnowledgeBase",
            "bedrock:GetAgentVersion",
            "bedrock:GetEvaluationJob",
            "bedrock:GetInferenceProfile",
```

```
            "bedrock:GetIngestionJob",
            "bedrock:GetPrompt",
            "bedrock:InvokeAgent",
            "bedrock:InvokeFlow",
            "bedrock:InvokeInlineAgent",
            "bedrock:InvokeModel",
            "bedrock:InvokeModelWithResponseStream",
            "bedrock:ListAgentActionGroups",
            "bedrock:ListAgentAliases",
            "bedrock:ListAgentKnowledgeBases",
            "bedrock:ListAgentVersions",
            "bedrock:ListEvaluationJobs",
            "bedrock:ListFoundationModels",
            "bedrock:ListIngestionJobs",
            "bedrock:ListPrompts",
            "bedrock:ListTagsForResource",
            "bedrock:Retrieve",
            "bedrock:RetrieveAndGenerate",
            "bedrock:StartIngestionJob",
            "bedrock:StopEvaluationJob",
            "bedrock:TagResource",
            "bedrock:UpdateAgentAlias",
            "cloudformation:DescribeStacks",
            "cloudformation:GetTemplate",
            "cloudwatch:DeleteAlarms",
            "cloudwatch:DescribeAlarms",
            "cloudwatch:GetMetricData",
            "cloudwatch:GetMetricStatistics",
            "cloudwatch:PutMetricAlarm",
            "cloudwatch:PutMetricData",
            "codecommit:BatchDescribeMergeConflicts",
            "codecommit:BatchGetCommits",
            "codecommit:BatchGetPullRequests",
            "codecommit:BatchGetRepositories",
            "codecommit:CreateBranch",
            "codecommit:CreateCommit",
            "codecommit:CreatePullRequest",
            "codecommit:DeleteBranch",
            "codecommit:DeleteFile",
            "codecommit:DescribeMergeConflicts",
            "codecommit:DescribePullRequestEvents",
            "codecommit:GetBlob",
            "codecommit:GetBranch",
            "codecommit:GetComment",
```

```
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
```

```
            "codecommit:UpdatePullRequestStatus",
            "codecommit:UpdatePullRequestTitle",
            "codecommit:UpdateRepositoryDescription",
            "codewhisperer:GenerateRecommendations",
            "datazone:CreateConnection",
            "datazone:DeleteConnection",
            "datazone:GetConnection",
            "datazone:GetDomain",
            "datazone:GetDomainExecutionRoleCredentials",
            "datazone:GetEnvironment",
            "datazone:GetEnvironmentBlueprintConfiguration",
            "datazone:GetProject",
            "datazone:GetUserProfile",
            "datazone:ListConnections",
            "datazone:ListEnvironmentBlueprints",
            "datazone:ListEnvironments",
            "datazone:ListProjects",
            "datazone:UpdateConnection",
            "dynamodb:BatchGetItem",
            "dynamodb:BatchWriteItem",
            "dynamodb:Scan",
            "dynamodb:Query",
            "dynamodb:DescribeBackup",
            "dynamodb:DescribeContributorInsights",
            "dynamodb:DescribeContinuousBackups",
            "dynamodb:DescribeEndpoints",
            "dynamodb:DescribeExport",
            "dynamodb:DescribeGlobalTable",
            "dynamodb:DescribeGlobalTableSettings",
            "dynamodb:DescribeImport",
            "dynamodb:DescribeKinesisStreamingDestination",
            "dynamodb:DescribeLimits",
            "dynamodb:DescribeReservedCapacity",
            "dynamodb:DescribeReservedCapacityOfferings",
            "dynamodb:DescribeStream",
            "dynamodb:DescribeTable",
            "dynamodb:DescribeTableReplicaAutoScaling",
            "dynamodb:DescribeTimeToLive",
            "dynamodb:GetItem",
            "dynamodb:GetRecords",
            "dynamodb:ListExports",
            "dynamodb:ListGlobalTables",
            "dynamodb:ListImports",
            "dynamodb:ListTables",
```

```
            "dynamodb:ListTagsOfResource",
            "dynamodb:PutItem",
            "dynamodb:PartiQLSelect",
            "dynamodb:PartiQLInsert",
            "dynamodb:PartiQLUpdate",
            "dynamodb:PartiQLDelete",
            "dynamodb:UpdateItem",
            "dynamodb:UpdateGlobalTable",
            "dynamodb:UpdateTable",
            "ec2:AttachNetworkInterface",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:CreateFleet",
            "ec2:CreateLaunchTemplate",
            "ec2:CreateLaunchTemplateVersion",
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:CreatePlacementGroup",
            "ec2:CreateSecurityGroup",
            "ec2:CreateTags",
            "ec2:CreateVpcEndpoint",
            "ec2:DeleteLaunchTemplate",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DeletePlacementGroup",
            "ec2:DeleteTags",
            "ec2:DescribeAccountAttributes",
            "ec2:DescribeCapacityReservations",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeImages",
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceTypeOfferings",
            "ec2:DescribeInstanceTypes",
            "ec2:DescribeLaunchTemplates",
            "ec2:DescribeNetworkAcls",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribePlacementGroups",
            "ec2:DescribeRouteTables",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeVolumes",
            "ec2:DescribeVolumeStatus",
            "ec2:DescribeVpcAttribute",
            "ec2:DescribeVpcEndpoints",
```

```
            "ec2:DescribeVpcs",
            "ec2:DetachNetworkInterface",
            "ec2:ModifyInstanceAttribute",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:RunInstances",
            "ec2:TerminateInstances",
            "ecr:BatchGetImage",
            "ecr:DescribeImages",
            "ecr:GetAuthorizationToken",
            "ecr:GetDownloadUrlForLayer",
            "elasticfilesystem:DescribeMountTargets",
            "elasticmapreduce:CreatePersistentAppUI",
            "elasticmapreduce:DescribeCluster",
            "elasticmapreduce:DescribePersistentAppUI",
            "elasticmapreduce:GetClusterSessionCredentials",
            "elasticmapreduce:GetManagedScalingPolicy",
            "elasticmapreduce:GetOnClusterAppUIPresignedURL",
            "elasticmapreduce:GetPersistentAppUIPresignedURL",
            "elasticmapreduce:ListBootstrapActions",
            "elasticmapreduce:ListClusters",
            "elasticmapreduce:ListInstanceFleets",
            "elasticmapreduce:ListInstanceGroups",
            "elasticmapreduce:ListInstances",
            "elasticmapreduce:ListReleaseLabels",
            "elasticmapreduce:ListSupportedInstanceTypes",
            "elasticmapreduce:TerminateJobFlows",
            "emr-serverless:AccessInteractiveEndpoints",
            "emr-serverless:AccessLivyEndpoints",
            "emr-serverless:GetApplication",
            "emr-serverless:GetDashboardForJobRun",
            "emr-serverless:GetJobRun",
            "emr-serverless:ListApplications",
            "emr-serverless:ListJobRunAttempts",
            "emr-serverless:ListJobRuns",
            "emr-serverless:StartApplication",
            "emr-serverless:StartJobRun",
            "emr-serverless:StopApplication",
            "glue:BatchCreatePartition",
            "glue:BatchDeletePartition",
            "glue:BatchDeleteTable",
            "glue:BatchDeleteTableVersion",
            "glue:BatchGetPartition",
            "glue:BatchGetTableOptimizer",
```

```
            "glue:BatchStopJobRun",
            "glue:BatchUpdatePartition",
            "glue:CancelDataQualityRuleRecommendationRun",
            "glue:CancelDataQualityRulesetEvaluationRun",
            "glue:CancelStatement",
            "glue:CreateBlueprint",
            "glue:CreateDatabase",
            "glue:CreateDataQualityRuleset",
            "glue:CreateJob",
            "glue:CreatePartition",
            "glue:CreatePartitionIndex",
            "glue:CreateSession",
            "glue:CreateTable",
            "glue:CreateWorkflow",
            "glue:DeleteBlueprint",
            "glue:DeleteColumnStatisticsForPartition",
            "glue:DeleteColumnStatisticsForTable",
            "glue:DeleteDatabase",
            "glue:DeleteDataQualityRuleset",
            "glue:DeleteJob",
            "glue:DeletePartition",
            "glue:DeletePartitionIndex",
            "glue:DeleteSession",
            "glue:DeleteTable",
            "glue:DeleteTableVersion",
            "glue:DeleteWorkflow",
            "glue:DescribeConnectionType",
            "glue:DescribeEntity",
            "glue:GetCatalog",
            "glue:GetCatalogImportStatus",
            "glue:GetCatalogs",
            "glue:GetClassifier",
            "glue:GetClassifiers",
            "glue:GetColumnStatisticsForPartition",
            "glue:GetColumnStatisticsForTable",
            "glue:GetColumnStatisticsTaskRun",
            "glue:GetColumnStatisticsTaskRuns",
            "glue:GetCompletion",
            "glue:GetConnection",
            "glue:GetConnections",
            "glue:GetDashboardUrl",
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetDataQualityModel",
```

```
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:GetEntityRecords",
        "glue:GetGeneratedCode",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:ListConnectionTypes",
        "glue:ListCrawls",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:ListEntities",
        "glue:ListSessions",
        "glue:ListStatements",
        "glue:ListTableOptimizerRuns",
        "glue:NotifyEvent",
        "glue:PassConnection",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:PutWorkflowRunProperties",
        "glue:ResumeWorkflowRun",
        "glue:RunStatement",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCompletion",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:StartJobRun",
```

```
            "glue:StartWorkflowRun",
            "glue:StopSession",
            "glue:StopWorkflowRun",
            "glue:TagResource",
            "glue:UntagResource",
            "glue:UpdateBlueprint",
            "glue:UpdateCatalog",
            "glue:UpdateColumnStatisticsForPartition",
            "glue:UpdateColumnStatisticsForTable",
            "glue:UpdateDataQualityRuleset",
            "glue:UpdateJob",
            "glue:UpdatePartition",
            "glue:UpdateTable",
            "glue:UpdateWorkflow",
            "glue:UseGlueStudio",
            "iam:CreateServiceLinkedRole",
            "iam:GetRole",
            "iam:ListRoles",
            "iam:PassRole",
            "kms:CreateGrant",
            "kms:Decrypt",
            "kms:DescribeKey",
            "kms:Encrypt",
            "kms:GenerateDataKey",
            "kms:GenerateDataKeyWithoutPlaintext",
            "kms:GetPublicKey",
            "kms:ListAliases",
            "kms:ListGrants",
            "kms:ReEncryptFrom",
            "kms:ReEncryptTo",
            "kms:RevokeGrant",
            "lakeformation:GetDataAccess",
            "lambda:InvokeFunction",
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams",
            "logs:FilterLogEvents",
            "logs:GetLogEvents",
            "logs:GetLogGroupFields",
            "logs:GetLogRecord",
            "logs:GetQueryResults",
            "logs:PutLogEvents",
            "logs:StartQuery",
```

```
            "logs:StopQuery",
            "pricing:GetProducts",
            "q:SendMessage",
            "q:StartConversation",
            "redshift-data:BatchExecuteStatement",
            "redshift-data:CancelStatement",
            "redshift-data:DescribeStatement",
            "redshift-data:DescribeTable",
            "redshift-data:ExecuteStatement",
            "redshift-data:GetStagingBucketLocation",
            "redshift-data:GetStatementResult",
            "redshift-data:ListDatabases",
            "redshift-data:ListSchemas",
            "redshift-data:ListStatements",
            "redshift-data:ListTables",
            "redshift-serverless:GetCredentials",
            "redshift-serverless:GetManagedWorkgroup",
            "redshift-serverless:GetNamespace",
            "redshift-serverless:GetWorkgroup",
            "redshift-serverless:ListNamespaces",
            "redshift-serverless:ListTagsForResource",
            "redshift-serverless:ListWorkgroups",
            "redshift:DescribeClusters",
            "redshift:DescribeTags",
            "redshift:GetClusterCredentialsWithIAM",
            "resource-groups:CreateGroup",
            "resource-groups:DeleteGroup",
            "resource-groups:GetGroupQuery",
            "resource-groups:ListGroupResources",
            "resource-groups:Tag",
            "s3:AbortMultipartUpload",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucketLocation",
            "s3:GetEncryptionConfiguration",
            "s3:GetObject*",
            "s3:ListBucket",
            "s3:ListBucketVersions",
            "s3:ListMultipartUploadParts",
            "s3:PutObject",
            "s3:PutObjectRetention",
            "s3:PutObjectTagging",
            "s3:ReplicateObject",
```

```
            "s3:RestoreObject",
            "sagemaker-mlflow:AccessUI",
            "sagemaker-mlflow:CreateExperiment",
            "sagemaker-mlflow:CreateModelVersion",
            "sagemaker-mlflow:CreateRegisteredModel",
            "sagemaker-mlflow:CreateRun",
            "sagemaker-mlflow:DeleteExperiment",
            "sagemaker-mlflow:DeleteModelVersion",
            "sagemaker-mlflow:DeleteModelVersionTag",
            "sagemaker-mlflow:DeleteRegisteredModel",
            "sagemaker-mlflow:DeleteRegisteredModelAlias",
            "sagemaker-mlflow:DeleteRegisteredModelTag",
            "sagemaker-mlflow:DeleteRun",
            "sagemaker-mlflow:DeleteTag",
            "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
            "sagemaker-mlflow:GetExperiment",
            "sagemaker-mlflow:GetExperimentByName",
            "sagemaker-mlflow:GetLatestModelVersions",
            "sagemaker-mlflow:GetMetricHistory",
            "sagemaker-mlflow:GetModelVersion",
            "sagemaker-mlflow:GetModelVersionByAlias",
            "sagemaker-mlflow:GetRegisteredModel",
            "sagemaker-mlflow:GetRun",
            "sagemaker-mlflow:ListArtifacts",
            "sagemaker-mlflow:LogBatch",
            "sagemaker-mlflow:LogInputs",
            "sagemaker-mlflow:LogMetric",
            "sagemaker-mlflow:LogModel",
            "sagemaker-mlflow:LogParam",
            "sagemaker-mlflow:RenameRegisteredModel",
            "sagemaker-mlflow:RestoreExperiment",
            "sagemaker-mlflow:RestoreRun",
            "sagemaker-mlflow:SearchExperiments",
            "sagemaker-mlflow:SearchModelVersions",
            "sagemaker-mlflow:SearchRegisteredModels",
            "sagemaker-mlflow:SearchRuns",
            "sagemaker-mlflow:SetExperimentTag",
            "sagemaker-mlflow:SetRegisteredModelAlias",
            "sagemaker-mlflow:SetRegisteredModelTag",
            "sagemaker-mlflow:SetTag",
            "sagemaker-mlflow:TransitionModelVersionStage",
            "sagemaker-mlflow:UpdateExperiment",
            "sagemaker-mlflow:UpdateModelVersion",
            "sagemaker-mlflow:UpdateRegisteredModel",
```

```
            "sagemaker-mlflow:UpdateRun",
            "sagemaker:AddAssociation",
            "sagemaker:AddTags",
            "sagemaker:BatchDescribeModelPackage",
            "sagemaker:BatchGetMetrics",
            "sagemaker:BatchPutMetrics",
            "sagemaker:CallPartnerAppApi",
            "sagemaker:CreateAction",
            "sagemaker:CreateApp",
            "sagemaker:CreateArtifact",
            "sagemaker:CreateAutoMLJob",
            "sagemaker:CreateAutoMLJobV2",
            "sagemaker:CreateContext",
            "sagemaker:CreateEndpoint",
            "sagemaker:CreateEndpointConfig",
            "sagemaker:CreateHyperParameterTuningJob",
            "sagemaker:CreateInferenceComponent",
            "sagemaker:CreateInferenceRecommendationsJob",
            "sagemaker:CreateModel",
            "sagemaker:CreateModelPackage",
            "sagemaker:CreateModelPackageGroup",
            "sagemaker:CreatePartnerAppPresignedUrl",
            "sagemaker:CreatePipeline",
            "sagemaker:CreatePresignedDomainUrl",
            "sagemaker:CreatePresignedMlflowTrackingServerUrl",
            "sagemaker:CreateProcessingJob",
            "sagemaker:CreateSpace",
            "sagemaker:CreateTrainingJob",
            "sagemaker:CreateTransformJob",
            "sagemaker:CreateUserProfile",
            "sagemaker:DeleteAction",
            "sagemaker:DeleteApp",
            "sagemaker:DeleteArtifact",
            "sagemaker:DeleteAssociation",
            "sagemaker:DeleteContext",
            "sagemaker:DeleteEndpoint",
            "sagemaker:DeleteEndpointConfig",
            "sagemaker:DeleteInferenceComponent",
            "sagemaker:DeleteModel",
            "sagemaker:DeleteModelPackage",
            "sagemaker:DeleteModelPackageGroup",
            "sagemaker:DeletePipeline",
            "sagemaker:DeleteSpace",
            "sagemaker:DeleteTags",
```

```
            "sagemaker:DeleteUserProfile",
            "sagemaker:DescribeAction",
            "sagemaker:DescribeApp",
            "sagemaker:DescribeArtifact",
            "sagemaker:DescribeAutoMLJob",
            "sagemaker:DescribeAutoMLJobV2",
            "sagemaker:DescribeContext",
            "sagemaker:DescribeDomain",
            "sagemaker:DescribeEndpoint",
            "sagemaker:DescribeEndpointConfig",
            "sagemaker:DescribeHyperParameterTuningJob",
            "sagemaker:DescribeImage",
            "sagemaker:DescribeImageVersion",
            "sagemaker:DescribeInferenceComponent",
            "sagemaker:DescribeInferenceRecommendationsJob",
            "sagemaker:DescribeMlflowTrackingServer",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeModelPackage",
            "sagemaker:DescribeModelPackageGroup",
            "sagemaker:DescribeOptimizationJob",
            "sagemaker:DescribePartnerApp",
            "sagemaker:DescribePipeline",
            "sagemaker:DescribePipelineDefinitionForExecution",
            "sagemaker:DescribePipelineExecution",
            "sagemaker:DescribeProcessingJob",
            "sagemaker:DescribeSpace",
            "sagemaker:DescribeTrainingJob",
            "sagemaker:DescribeTransformJob",
            "sagemaker:DescribeTrialComponent",
            "sagemaker:DescribeUserProfile",
            "sagemaker:GetSearchSuggestions",
            "sagemaker:InvokeEndpoint",
            "sagemaker:InvokeEndpointAsync",
            "sagemaker:InvokeEndpointWithResponseStream",
            "sagemaker:ListApps",
            "sagemaker:ListArtifacts",
            "sagemaker:ListAssociations",
            "sagemaker:ListAutoMLJobs",
            "sagemaker:ListCandidatesForAutoMLJob",
            "sagemaker:ListContexts",
            "sagemaker:ListDomains",
            "sagemaker:ListEndpointConfigs",
            "sagemaker:ListEndpoints",
            "sagemaker:ListHubContents",
```

```
            "sagemaker:ListHubs",
            "sagemaker:ListHyperParameterTuningJobs",
            "sagemaker:ListImageVersions",
            "sagemaker:ListInferenceComponents",
            "sagemaker:ListMlflowTrackingServers",
            "sagemaker:ListModelMetadata",
            "sagemaker:ListModelPackageGroups",
            "sagemaker:ListModelPackages",
            "sagemaker:ListModels",
            "sagemaker:ListPartnerApps",
            "sagemaker:ListPipelineExecutions",
            "sagemaker:ListPipelineExecutionSteps",
            "sagemaker:ListPipelineParametersForExecution",
            "sagemaker:ListPipelines",
            "sagemaker:ListProcessingJobs",
            "sagemaker:ListSpaces",
            "sagemaker:ListTags",
            "sagemaker:ListTrainingJobs",
            "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
            "sagemaker:ListTransformJobs",
            "sagemaker:ListUserProfiles",
            "sagemaker:QueryLineage",
            "sagemaker:RetryPipelineExecution",
            "sagemaker:Search",
            "sagemaker:SendPipelineExecutionStepFailure",
            "sagemaker:SendPipelineExecutionStepSuccess",
            "sagemaker:StartMlflowTrackingServer",
            "sagemaker:StartPipelineExecution",
            "sagemaker:StopAutoMLJob",
            "sagemaker:StopHyperParameterTuningJob",
            "sagemaker:StopMlflowTrackingServer",
            "sagemaker:StopPipelineExecution",
            "sagemaker:StopProcessingJob",
            "sagemaker:StopTrainingJob",
            "sagemaker:StopTransformJob",
            "sagemaker:UpdateEndpoint",
            "sagemaker:UpdateEndpointWeightsAndCapacities",
            "sagemaker:UpdateInferenceComponentRuntimeConfig",
            "sagemaker:UpdateMlflowTrackingServer",
            "sagemaker:UpdateModelPackage",
            "sagemaker:UpdatePipeline",
            "sagemaker:UpdatePipelineExecution",
            "sagemaker:UpdateSpace",
            "sagemaker:UpdateTrainingJob",
```

```
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:ListSecrets",
        "secretsmanager:PutSecretValue",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:GetQSqlPromptQuotas",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:ListTabs",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:PutTab",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "sts:AssumeRole",
        "sts:GetCallerIdentity",
        "sts:SetSourceIdentity",
        "sts:TagSession",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioProjectUserRolePolicy

描述：Amazon SageMaker Studio 會為專案使用者建立 IAM 角色，以執行資料分析、人工智慧和機器學習動作，並在建立這些角色時使用此政策來定義許可。

SageMakerStudioProjectUserRolePolicy 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioProjectUserRolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2024 年 11 月 20 日，UTC 21：59
- 編輯時間：2026 年 3 月 2 日 20：27 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy

政策版本

政策版本： v63 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCommit",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
```

```
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CodeCommitKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        }
      }
    },
    {
      "Sid" : "CodeWhisperer",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGlueCreateEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGlueCreateEniOnSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowGlueCreateEniOnSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManageGlueEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/aws-glue-service-resource" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAttachGlueEniOnInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeGlueEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueKernelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "GlueTagSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:GetSession",
        "glue:ListStatements",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:GetStatement",
```

```
        "glue:StopSession",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:DeleteDataQualityRuleset",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:UpdateDataQualityRuleset",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:BatchGetJobs",
        "glue:GetJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
```

```
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueListJobsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueVisualETLPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetGeneratedCode"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCompletionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*",
        "arn:aws:glue:*:*:job/*"
```

```
      ]
    },
    {
      "Sid" : "GlueJobRunnerSessionLogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws-glue/*"
    },
    {
      "Sid" : "EC2TagsPermissionsForGlue",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        },
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/DefaultGlueCatalogKmsKeyId}",
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrServerlessInteractivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication",
        "emr-serverless:StopApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EmrServerlessJobAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun"
      ],
      "Resource" : [
        "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowActionsForTaggedEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowListEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowUiApiAccess",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : [
        "arn:aws:airflow:*:*:role/DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}/User"
      ]
    },
    {
```

```
      "Sid" : "AirflowCloudwatchLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:airflow-DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}-*"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AmazonMWAA"
        }
      }
    },
    {
      "Sid" : "GlueJobCloudwatchPutMetricActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "Glue",
            "AWS/Glue"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowSqsActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:airflow-celery-*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:GetPublicKey",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountDecryptKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaFederatedCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
"arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessLevelControlS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketAcl",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
```

```
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "DZDomainKMSKeyXAcctPerm",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/DomainKmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:datazone:domainId" : "${aws:PrincipalTag/
AmazonDataZoneDomain}"
        },
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListLogGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueJobLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/output",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/error",
```

```
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/output:log-
stream:*",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/error:log-
stream:*"
      ]
    },
    {
      "Sid" : "ProjectLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
```

```
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "DefaultAthenaDataCatalogPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:datacatalog/AwsDataCatalog",
        "arn:aws:athena:*:*:datacatalog/awsdatacatalog"
      ]
    },
    {
      "Sid" : "AthenaListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneUserPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "datazone:PostLineageEvent"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/${aws:PrincipalTag/
AmazonDataZoneDomain}"
```

```
    },
    {
      "Sid" : "GlueGetDefaultDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowGlueGetDatabasesExceptDefault",
      "Effect" : "Allow",
      "Action" : "glue:GetDatabases",
      "NotResource" : "arn:aws:glue:*:*:database/default",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueListDatabasesOnNoDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueFileUploadPermissions",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:UseGlueStudio"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Sid" : "GlueProjectConnectionPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnection",
        "glue:GetConnections"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueGetConnectionOnlyOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:DeleteDatabase",
```

```
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueCrawlerPermissions",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueDefaultCatalogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueNonDefaultCatalogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "LakeFormationPermissionForDataLakeAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess",
        "lakeformation:GetResourceLFTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAssumeAccessRole",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "TagSessionForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "AmazonDataZoneDomain"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${aws:PrincipalTag/
AmazonDataZoneDomain}"
        }
      }
    },
    {
      "Sid" : "SetContextForTrustedIdentityPropagation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:sts::*:self"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "StsContext",
      "Effect" : "Allow",
      "Action" : "sts:SetContext",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        }
      }
    },
    {
      "Sid" : "FederatedDataConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
```

```
        }
      }
    },
    {
      "Sid" : "UnRestrictedAccessForGlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleOnProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/RoleName}",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "airflow-serverless.amazonaws.com",
            "sagemaker.amazonaws.com",
            "glue.amazonaws.com",
            "airflow.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "scheduler.amazonaws.com",
            "access-grants.s3.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "SQLWorkBenchActionsWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletion*",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:*QCustomContext",
        "sqlworkbench:GetQSql*",
        "sqlworkbench:GetSchemaInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SQLWorkBenchActions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:AssociateNotebookWithTab",
      "Resource" : "arn:*:sqlworkbench:*:*:notebook/*"
    },
    {
      "Sid" : "SQLWorkBenchNotebookActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateNotebook*",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook*",
        "sqlworkbench:DeleteNotebook*",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
```

```
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowAccessExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
```

```
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessWorkgroupWithResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeCredentials",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:GetManagedEndpointSessionCredentials",
        "redshift-serverless:GetCredentials",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
```

```
      "Sid" : "RedshiftDataActionsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RedshifServerlessCredentialsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "redshift-data.amazonaws.com",
            "sqlworkbench.amazonaws.com"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowTagGetResources",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGetSecretForRedShift",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRClusterWithDataZoneTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
```

```
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRClusterInfoPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRGetClusterSessionCredentials",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetClusterSessionCredentials"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ArnLike" : {
```

```
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "EmrContainersSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EMRPersistentAppUI",
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "elasticmapreduce:GetPersistentAppUIPresignedURL"
      ],
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "KmsWithEncrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
```

```
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "scheduler.*.amazonaws.com",
            "glue.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "EBDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "emr-serverless.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "KmsManagement",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "scheduler.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "AwsOwnedKmsKeyPermissions",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsManagement",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
```

```
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2PermissionsForNotebookExecution",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeBedrockModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        },
```

```
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        },
        "ArnLike" : {
          "bedrock:InferenceProfileArn" : "arn:aws:bedrock:*:*:application-inference-
profile/*"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModelAppInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockInvokeModelAppInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AccessBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
```

```
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockResourceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateAgentAlias",
        "bedrock:CreateBlueprint",
        "bedrock:CreateBlueprintVersion",
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteBlueprint",
        "bedrock:DeleteDataAutomationProject",
        "bedrock:DeletePrompt",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentVersion",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetEvaluationJob",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
        "bedrock:InvokeAgent",
        "bedrock:InvokeDataAutomationAsync",
        "bedrock:InvokeFlow",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentVersions",
        "bedrock:ListIngestionJobs",
```

```
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
        "bedrock:UpdateAgentAlias",
        "bedrock:UpdateBlueprint",
        "bedrock:UpdateDataAutomationProject",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases"
      ],
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateEvaluationJobForFoundationModelPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "BedrockCreateEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*::foundation-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "InvokeDataAutomationAsyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeDataAutomationAsync"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:data-automation-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BedrockInvokeInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
```

```
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockNoResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListEvaluationJobs",
        "bedrock:RetrieveAndGenerate",
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRoleToBedrockPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
```

```
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "ProjectUserTag*"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockTagResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonBedrockManaged",
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "KmsViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "kms:EncryptionContextKeys" : [
            "aws:bedrock*:arn",
            "aws:bedrock:guardrail-id"
          ]
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AccessSecretKmsPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*"
        }
      }
    },
```

```
    {
      "Sid" : "KmsViaSecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:CalledViaFirst" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaInvokeFunctionViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:CalledViaFirst" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GetDataZoneEnvironmentCloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CloudFormationGetDataZoneEnvironmentStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionGetSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionLambdaLogsPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/athenafederatedcatalog*"
    },
    {
      "Sid" : "FederatedConnectionDDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConnectionEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionDeleteENIPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionDescribeENIPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:BatchDeleteImage",
        "ecr:ListTagsForResource",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:UploadLayerPart"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateECRRepositoryPermission",
      "Effect" : "Allow",
      "Action" : "ecr:CreateRepository",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRTagResourcePermission",
      "Effect" : "Allow",
```

```
      "Action" : "ecr:TagResource",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRUntagResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
```

```
        "lakeformation:ListPermissions",
        "lakeformation:DescribeResource",
        "ram:GetResourceShareInvitations",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:UpdateDataCellsFilter",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "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" : "CrossAccountRAMResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
```

```
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RAMGetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*",
            "DataZoneS3AG*"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:GetSchedule",
```

```
        "scheduler:UpdateSchedule",
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightFolderAndDataSourceResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:ListFolderMembers"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:folder/*",
        "arn:aws:quicksight:*:*:datasource/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightOtherResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeUser",
        "quicksight:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ]
    },
    {
      "Sid" : "ManagePassDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PassDataSource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageCreateDataSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:TagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
```

```
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateFolderMembership",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateFolderMembership"
      ],
      "Resource" : "arn:aws:quicksight:*:*:folder/sagemaker-*-assets",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneAssetsFolder" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:InvokeMcp",
        "sagemaker-unified-studio-mcp:CallReadOnlyTool",
        "sagemaker-unified-studio-mcp:CallPrivilegedTool"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SageMakerStudioQueryExecutionRolePolicy

描述：Amazon SageMaker Studio 會在聯合連線上執行查詢執行時使用此政策。

`SageMakerStudioQueryExecutionRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioQueryExecutionRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 1 月 31 日 19：52 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioQueryExecutionRolePolicy`

政策版本

政策版本： v6 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "GlueGetConnectionOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueGetConnectionsForProject",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "arn:aws:glue:*:*:connection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3GetObjectForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/dzd*/*/dev/sys/athena/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "S3ListBucketOwnershipCheckForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SageMakerStudioUserIAMConsolePolicy

描述：透過 AWS 管理主控台 和 SDK 提供 Amazon SageMaker Unified Studio 的個別設定權限。允許啟動 SageMaker Unified Studio 入口網站。

`SageMakerStudioUserIAMConsolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioUserIAMConsolePolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 18 日，UTC 22：49
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioUserIAMConsolePolicy

政策版本

政策版本： v9 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListDomains",
        "datazone:GetDomain",
        "datazone:GetUserProfile",
        "datazone:ListProjects",
        "datazone:ListProjectProfiles",
        "datazone:CreateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:GetIamPortalLoginUrl",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironments",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentCredentials",
```

```
        "datazone:GetGroupProfile",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "datazone:ListProjectMemberships"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SageMakerStudioUserIAMDefaultExecutionPolicy

描述：搭配 SageMaker Unified Studio 使用 IAM 角色的執行政策。允許使用者存取本機帳戶中的資源（不包括對資料資源的存取），以使用 IAM 為基礎的 SageMaker Unified Studio。

`SageMakerStudioUserIAMDefaultExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SageMakerStudioUserIAMDefaultExecutionPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 18 日 17：19 UTC
- 編輯時間：2026 年 3 月 11 日 17：42 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy`

政策版本

政策版本： v22（預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:CreateNotebook",
        "datazone:UpdateNotebook",
        "datazone:DeleteNotebook",
        "datazone:CreateCell",
        "datazone:UpdateCell",
```

```
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartNotebookCompute",
        "datazone:StopNotebookCompute",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:InvokeMcp",
        "sagemaker-unified-studio-mcp:CallReadOnlyTool",
        "sagemaker-unified-studio-mcp:CallPrivilegedTool"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "Q",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "SageMakerUserTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
```

```
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerPrivateSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:CreateSpace",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
```

```
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Batch*",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:*MlflowApp*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringNotLike" : {
```

```
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        }
      }
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:CreateCatalog",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
```

```
        "glue:UseGlueStudio",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:*Job*",
        "glue:TestConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
```

```
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SQLWorkBench",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/
AmazonDataZonePassedRolePath}",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "S3CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:Get*",
        "scheduler:List*",
        "scheduler:UpdateSchedule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
```

```
        "athena:BatchGet*",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:Get*",
        "athena:ImportNotebook",
        "athena:List*",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TagResource",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
```

```
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "PrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codeconnections:ListConnections",
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codeconnections:ListTagsForResource",
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
```

```
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
```

```
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
```

```
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AccessProjectS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject*",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject*",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/AmazonDataZoneProjectBucket}/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProjectBucket" : ""
```

```
        }
      }
    },
    {
      "Sid" : "EMRServerless",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:ListApplications",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:AccessLivyEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SageMakerStudioUserIAMPermissiveExecutionPolicy

描述：搭配 SageMaker Unified Studio 使用 IAM 角色的執行政策。允許使用者存取您帳戶中的資源（包括對 S3、Glue、CloudWatch Logs 等資料服務中的所有 APIs 的廣泛存取），以使用 IAM 為基礎的 SageMaker Unified Studio。

`SageMakerStudioUserIAMPermissiveExecutionPolicy` 是 AWS 受管政策。

使用此政策

您可以將 SageMakerStudioUserIAMPermissiveExecutionPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2025 年 8 月 18 日 17：19 UTC
- 編輯時間：2026 年 3 月 5 日 17：42 UTC
- ARN: arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy

政策版本

政策版本： v16 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*",
        "s3tables:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
```

```
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
```

```
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:CreateNotebook",
        "datazone:UpdateNotebook",
        "datazone:DeleteNotebook",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartNotebookCompute",
        "datazone:StopNotebookCompute",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
```

```
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codeconnections:ListConnections",
        "codeconnections:GetConnection",
```

```
        "codeconnections:GetHost",
        "codeconnections:ListTagsForResource",
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
```

```
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
```

```
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SecretsManagerReadWrite

描述：透過 提供 AWS Secrets Manager 的讀取/寫入存取權 AWS 管理主控台。注意：這會排除 IAM 動作，因此如果需要輪換組態，請結合 IAMFullAccess。

SecretsManagerReadWrite 是 AWS 受管政策。

使用此政策

您可以將 SecretsManagerReadWrite 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 4 月 4 日 18：05 UTC
- 編輯時間：2024 年 2 月 22 日 18：12 UTC
- ARN: arn:aws:iam::aws:policy/SecretsManagerReadWrite

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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-*/*"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SecurityAgentWebAppAPIPolicy

描述：提供已驗證使用者存取 Security Agent Web Application 的許可，以設定和執行自動化安全滲透測試。此政策可讓使用者管理 pentest、檢視問題清單、監控測試執行，以及與安全測試操作所需的 AWS 資源互動。

`SecurityAgentWebAppAPIPolicy` 是 AWS 受管政策。

使用此政策

您可以將 `SecurityAgentWebAppAPIPolicy` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2025 年 12 月 2 日 15：04 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SecurityAgentWebAppAPIPolicy`

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentInstances",
        "securityagent:ListControls"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentInstances",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetSecurityTestContentMetadata",
        "securityagent:BatchGetTasks",
        "securityagent:CreateDocumentReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:DeleteDocumentReview",
        "securityagent:GetArtifact",
        "securityagent:GetCodeReviewTask",
        "securityagent:GetDocReviewTask",
        "securityagent:GetDocumentReview",
```

```
        "securityagent:GetDocumentReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListControls",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDocumentReviewComments",
        "securityagent:ListDocumentReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListTasks",
        "securityagent:StartCodeRemediation",
        "securityagent:StartPentestExecution",
        "securityagent:StopPentestExecution",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-instance*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

SecurityAgentWebAppPolicy

描述：提供已驗證使用者存取 Security Agent Web Application 的許可，以設定和執行自動化安全滲透測試。此政策可讓使用者管理 pentest、檢視問題清單、監控測試執行，以及與安全測試操作所需的 AWS 資源互動。

SecurityAgentWebAppPolicy 是 AWS 受管政策。

使用此政策

您可以將 SecurityAgentWebAppPolicy 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2026 年 2 月 5 日 20：19 UTC
- 編輯時間：2026 年 2 月 12 日 18：01 UTC
- ARN: arn:aws:iam::aws:policy/SecurityAgentWebAppPolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentSpaces",
        "securityagent:ListSecurityRequirements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentSpaceAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentSpaces",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetPentestJobContentMetadata",
        "securityagent:BatchGetPentestJobTasks",
        "securityagent:CreateDesignReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:GetArtifact",
        "securityagent:DeleteDesignReview",
        "securityagent:GetDesignReview",
        "securityagent:GetDesignReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListSecurityRequirements",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDesignReviewComments",
        "securityagent:ListDesignReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListPentestJobTasks",
        "securityagent:StartCodeRemediation",
        "securityagent:StartPentestJob",
        "securityagent:StopPentestJob",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-space*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

SecurityAudit

描述：安全稽核範本授予讀取安全組態中繼資料的存取權。它適用於稽核 組態的軟體 AWS 帳戶。

SecurityAudit 是 AWS 受管政策。

使用此政策

您可以將 SecurityAudit 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2026 年 3 月 2 日 17：12 UTC
- ARN: arn:aws:iam::aws:policy/SecurityAudit

政策版本

政策版本： v85 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
```

```
        "apprunner:ListVpcIngressConnections",
        "appsync:GetApiCache",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager: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:DescribeGlobalSettings",
        "backup:DescribeRegionSettings",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupVaults",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetCustomModel",
        "bedrock:GetFlowAlias",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetImportedModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelImportJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:GetProvisionedModelThroughput",
```

```
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListImportedModels",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListMarketplaceModelEndpoints",
        "bedrock:ListModelCopyJobs",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelImportJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:ListTagsForResource",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
```

```
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
```

```
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListTagsForResource",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:GetResourcePolicy",
        "codebuild:ListProjects",
        "codebuild:ListSourceCredentials",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
```

```
        "cognito-sync:Describe*",
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListApprovedOrigins",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListLexBots",
        "connect:ListSecurityKeys",
        "databrew:DescribeDataset",
        "databrew:DescribeProject",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "dataexchange:ListDataSets",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
        "datasync:Describe*",
        "datasync:List*",
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
```

```
        "devicefarm:ListProjects",
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
```

```
        "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:ListAccessEntries",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks:ListTagsForResource",
        "eks:ListUpdates",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
```

```
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elastictranscoder:ListPipelines",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdNamespace",
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
```

```
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoints",
        "glue:GetJobs",
        "glue:GetResourcePolicy",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTags",
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribeMalwareScans",
        "guardduty:DescribeOrganizationConfiguration",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "health:DescribeAffectedAccountsForOrganization",
        "health:DescribeAffectedEntities",
        "health:DescribeAffectedEntitiesForOrganization",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEventDetails",
        "health:DescribeEventDetailsForOrganization",
        "health:DescribeEvents",
        "health:DescribeEventsForOrganization",
        "health:DescribeEventTypes",
        "health:DescribeHealthServiceStatusForOrganization",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "identitystore:DescribeGroupMembership",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
```

```
        "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:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeLimits",
        "kinesis:DescribeStream",
```

```
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "lex:DescribeBot",
        "lex:DescribeResourcePolicy",
        "lex:ListBots",
        "license-manager:List*",
        "lightsail:GetBuckets",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancers",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
```

```
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:DescribeMLModels",
        "macie2:ListFindings",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:ListContainers",
        "memorydb:DescribeClusters",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
```

```
            "nimble:ListStudios",
            "opsworks-cm:DescribeServers",
            "opsworks:DescribeStacks",
            "organizations:Describe*",
            "organizations:List*",
            "pcs:GetCluster",
            "pcs:GetComputeNodeGroup",
            "pcs:GetQueue",
            "pcs:ListClusters",
            "pcs:ListComputeNodeGroups",
            "pcs:ListQueues",
            "pcs:ListTagsForResource",
            "personalize:DescribeDatasetGroup",
            "personalize:ListDatasetGroups",
            "private-networks:ListNetworks",
            "profile:GetDomain",
            "profile:ListDomains",
            "profile:ListIntegrations",
            "qbusiness:ListApplications",
            "qbusiness:ListDataSources",
            "qbusiness:ListDataSourceSyncJobs",
            "qbusiness:ListDocuments",
            "qbusiness:ListGroups",
            "qbusiness:ListIndices",
            "qbusiness:ListPlugins",
            "qbusiness:ListRetrievers",
            "qbusiness:ListSubscriptions",
            "qbusiness:ListTagsForResource",
            "qbusiness:ListWebExperiences",
            "qldb:DescribeJournalS3Export",
            "qldb:DescribeLedger",
            "qldb:ListJournalS3Exports",
            "qldb:ListJournalS3ExportsForLedger",
            "qldb:ListLedgers",
            "quicksight:Describe*",
            "quicksight:List*",
            "ram:GetResourceShares",
            "ram:List*",
            "rds:Describe*",
            "rds:DownloadDBLogFilePortion",
            "rds:ListTagsForResource",
            "redshift-serverless:GetNamespace",
            "redshift-serverless:ListTagsForResource",
            "redshift-serverless:ListWorkgroups",
```

```
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrantsInstanceResourcePolicy",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
```

```
            "s3:GetLifecycleConfiguration",
            "s3:GetMetricsConfiguration",
            "s3:GetMultiRegionAccessPoint",
            "s3:GetMultiRegionAccessPointPolicy",
            "s3:GetMultiRegionAccessPointPolicyStatus",
            "s3:GetObjectAcl",
            "s3:GetObjectTagging",
            "s3:GetObjectVersionAcl",
            "s3:GetReplicationConfiguration",
            "s3:GetStorageLensConfiguration",
            "s3:GetStorageLensGroup",
            "s3:ListAccessGrants",
            "s3:ListAccessGrantsInstances",
            "s3:ListAccessPoints",
            "s3:ListAccessPointsForObjectLambda",
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "s3:ListCallerAccessGrants",
            "s3:ListJobs",
            "s3:ListMultiRegionAccessPoints",
            "s3:ListStorageLensConfigurations",
            "s3:ListStorageLensGroups",
            "s3express:GetBucketPolicy",
            "s3express:GetEncryptionConfiguration",
            "s3express:ListAllMyDirectoryBuckets",
            "s3tables:GetNamespace",
            "s3tables:GetTableBucketMaintenanceConfiguration",
            "s3tables:GetTableBucketPolicy",
            "s3tables:GetTableMaintenanceConfiguration",
            "s3tables:GetTablePolicy",
            "s3tables:ListNamespaces",
            "s3tables:ListTableBuckets",
            "s3tables:ListTables",
            "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:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "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:GetAccount",
        "ses:GetAccountSendingEnabled",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetIdentityDkimAttributes",
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListDedicatedIpPools",
        "ses:ListIdentities",
        "ses:ListIdentityPolicies",
        "ses:ListReceiptFilters",
```

```
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting",
        "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:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:DescribeApplicationProvider",
        "sso:DescribeInstance",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeRegion",
        "sso:DescribeTrustedTokenIssuer",
```

```
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:GetApplicationAuthenticationMethod",
        "sso:GetApplicationGrant",
        "sso:GetApplicationSessionConfiguration",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListAccountAssignmentCreationStatus",
        "sso:ListAccountAssignmentDeletionStatus",
        "sso:ListAccountAssignments",
        "sso:ListAccountAssignmentsForPrincipal",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListApplicationAccessScopes",
        "sso:ListApplicationAssignments",
        "sso:ListApplicationAssignmentsForPrincipal",
        "sso:ListApplicationAuthenticationMethods",
        "sso:ListApplicationGrants",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationInstances",
        "sso:ListApplicationProviders",
        "sso:ListApplications",
        "sso:ListApplicationTemplates",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListDirectoryAssociations",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetProvisioningStatus",
        "sso:ListPermissionSets",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListRegions",
        "sso:ListTagsForResource",
        "sso:ListTrustedTokenIssuers",
        "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*",
        "voiceid:DescribeDomain",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
```

```
        "waf-regional:ListTagsForResource",
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAssistant",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
```

```
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制

- 開始使用 AWS 受管政策並邁向最低權限許可

SecurityLakeResourceManagementServiceRolePolicy

描述：提供管理 Security Lake 所建立資源的存取權。

SecurityLakeResourceManagementServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 11 月 14 日 22：10 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SecurityLakeResourceManagementServiceRolePolicy

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AmazonSecurityLake-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeLambdaConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:PutFunctionConcurrency",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetRuntimeManagementConfig",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:PublishVersion",
        "lambda:DeleteFunctionConcurrency",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetAlias",
        "lambda:GetPolicy",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeletePartitionUpdaterLambda",
      "Effect" : "Allow",
      "Action" : "lambda:DeleteFunction",
      "Resource" :
"arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListLambdaEventSourceMappings",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaEventSourceMapping",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateEventSourceMapping"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "lambda:FunctionArn" :
"arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
```

```
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaConfigs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:GetTables",
        "glue:UpdateTable",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeConfigurationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
```

```
        "s3:PutObject",
        "s3:GetObjectAttributes",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCompactionAndManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadSecurityLakeLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetQueryResults",
```

```
        "logs:GetLogRecord"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeSQSQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:StartMessageMoveTask",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ChangeMessageVisibility",
        "sqs:ListMessageMoveTasks",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake_*",
        "arn:aws:sqs:*:*:AmazonSecurityLakeManager-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

SecurityLakeServiceLinkedRole

描述：此政策授予代表您操作 Amazon Security Lake 服務的許可

`SecurityLakeServiceLinkedRole` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2022 年 11 月 29 日 14：03 UTC
- 編輯時間：2024 年 4 月 19 日 16：00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeOrgAccounts",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*"
      ]
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
    },
    {
      "Sid" : "AllowListServiceLinkedChannel",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAnyVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowWafLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "wafv2:LogScope" : "SecurityLake"
        }
      }
    },
    {
      "Sid" : "AllowPutLoggingConfiguration",
```

```
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
        }
      }
    },
    {
      "Sid" : "ListWebACLs",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListWebACLs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ServerMigration_ServiceRole

描述：允許 AWS Server Migration Service 將 VMs 遷移至 EC2 的許可：允許 Server Migration Service 將遷移的資源放置到客戶的 EC2 帳戶中。

`ServerMigration_ServiceRole` 是 AWS 受管政策。

使用此政策

您可以將 `ServerMigration_ServiceRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 8 月 11 日 20：41 UTC
- 編輯時間：2020 年 10 月 15 日 17：26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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-*/*"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ServerMigrationConnector

描述：允許 AWS Server Migration Connector 將 VMs許可。 EC2 允許與 AWS Server Migration Service 通訊、從 'sms-b-' 和 'import-to-ec2-' 開始對 S3 儲存貯體的讀取/寫入存取 AWS，以及用於 AWS Server Migration Connector 升級的儲存貯體、使用 的 AWS Server Migration Connector 註冊，以及上傳至其中的指標 AWS。

`ServerMigrationConnector` 是 AWS 受管政策。

使用此政策

您可以將 `ServerMigrationConnector` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策

- 建立時間：2016 年 10 月 24 日，UTC 21：45
- 編輯時間：2016 年 10 月 24 日，UTC 21：45
- ARN: arn:aws:iam::aws:policy/ServerMigrationConnector

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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-*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ServerMigrationServiceConsoleFullAccess

描述：使用 Server Migration Service Console 的所有功能所需的許可

`ServerMigrationServiceConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ServerMigrationServiceConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2020 年 5 月 9 日 17：18 UTC
- 編輯時間：2020 年 7 月 20 日，22：00 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ServerMigrationServiceLaunchRole

描述：允許 AWS Server Migration Service 建立和更新相關 AWS 資源到客戶 AWS 帳戶 啟動遷移伺服器和應用程式的許可。

`ServerMigrationServiceLaunchRole` 是 AWS 受管政策。

使用此政策

您可以將 `ServerMigrationServiceLaunchRole` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2018 年 11 月 26 日 19：53 UTC
- 編輯時間：2020 年 10 月 15 日 17：29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ServerMigrationServiceRoleForInstanceValidation

描述：允許 AWS SMS 執行已使用資料驗證指令碼並將指令碼成功/失敗傳回 SMS 的許可

ServerMigrationServiceRoleForInstanceValidation 是 AWS 受管政策。

使用此政策

您可以將 ServerMigrationServiceRoleForInstanceValidation 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2020 年 7 月 20 日，UTC 22：25
- 編輯時間：2020 年 7 月 20 日，22：25 UTC
- ARN: arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ServiceQuotasFullAccess

描述：提供 Service Quotas 的完整存取權

`ServiceQuotasFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `ServiceQuotasFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2019 年 6 月 24 日 15：44 UTC
- 編輯時間：2021 年 2 月 4 日 21：29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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"
        }
      }
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ServiceQuotasReadOnlyAccess

描述：提供 Service Quotas 的唯讀存取權

`ServiceQuotasReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 ServiceQuotasReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2019 年 6 月 24 日 15：31 UTC
- 編輯時間：2026 年 2 月 12 日 18：00 UTC
- ARN: arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess

政策版本

政策版本： v5 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "servicequotas:GetAutoManagementConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:GetNotificationConfiguration",
        "notifications:GetEventRule",
        "notifications:ListNotificationHubs",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:GetEmailContact",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackChannelConfigurations",
        "consoleapp:ListDeviceIdentities",
        "consoleapp:GetDeviceIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

ServiceQuotasServiceRolePolicy

描述：允許 Service Quotas 代表您建立支援案例

`ServiceQuotasServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 5 月 22 日，UTC 20：44
- 編輯時間：2019 年 6 月 24 日 14：52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

SignInLocalDevelopmentAccess

描述：提供 AWS 透過 AWS 登入服務以程式設計方式存取 的許可，包括開發人員工具和應用程式的 OAuth2 權杖建立。

`SignInLocalDevelopmentAccess` 是 AWS 受管政策。

使用此政策

您可以將 `SignInLocalDevelopmentAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2025 年 11 月 19 日 18：34 UTC
- 編輯時間：2026 年 2 月 12 日 17：59 UTC
- ARN: `arn:aws:iam::aws:policy/SignInLocalDevelopmentAccess`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:oauth2/public-client/*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SimpleWorkflowFullAccess

描述：提供 Simple Workflow 組態服務的完整存取權。

`SimpleWorkflowFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `SimpleWorkflowFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2015 年 2 月 6 日 18：41 UTC
- 編輯時間：2015 年 2 月 6 日 18：41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SMSVoiceServiceRolePolicy

描述：允許 SMSVoice 代表您將指標發佈至 CloudWatch

`SMSVoiceServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策

- 建立時間：2024 年 11 月 14 日 17：04 UTC
- 編輯時間：2024 年 11 月 14 日 17：04 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SMSVoiceServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SMSVoice"
        }
      }
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SplitCostAllocationDataServiceRolePolicy

描述：如果適用，允許分割成本分配資料擷取 AWS Organizations 資訊，並為客戶選擇加入的分割成本分配資料服務收集遙測資料。

SplitCostAllocationDataServiceRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 4 月 16 日 16：05 UTC
- 編輯時間：2024 年 4 月 16 日 16：05 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonManagedServiceForPrometheusAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aps:ListWorkspaces",
        "aps:QueryMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SSMQuickSetupRolePolicy

描述：提供許可來檢查快速設定組態運作狀態、確保參數和佈建資源的一致使用，以及在偵測到偏離時修復資源。

SSMQuickSetupRolePolicy 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2024 年 6 月 25 日 15：20 UTC
- 編輯時間：2024 年 11 月 18 日 13：06 UTC
- ARN: arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMResourceDataSyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMResourceDataSyncGetOpsSummaryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
    },
    {
      "Sid" : "SSMResourceDataSyncManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*",
      "Condition" : {
        "StringEquals" : {
          "ssm:SyncType" : "SyncFromSource"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "QuickSetupSSMDocumentsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
        "arn:aws:ssm:*:*:document/*-AWSQuickSetupType-*"
      ]
    },
    {
      "Sid" : "OrganizationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedServicesForAccount"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupStackSetReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*"
      ]
```

```
    },
    {
      "Sid" : "QuickSetupStackSetDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset-target/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuickSetupCfnStacksDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SupportUser

描述：此政策授予許可，以對 中的問題進行故障診斷和解決 AWS 帳戶。此政策也允許使用者聯絡 AWS 支援以建立和管理案例。

SupportUser 是 AWS 受管政策。

使用此政策

您可以將 SupportUser 連接至使用者、群組與角色。

政策詳細資訊

- 類型：任務函數政策
- 建立時間：2016 年 11 月 10 日 17：21 UTC
- 編輯時間：2026 年 2 月 12 日 18：03 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SupportUser

政策版本

政策版本： v11 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

SystemAdministrator

描述：授予應用程式和開發操作所需的資源所需的完整存取許可。

SystemAdministrator 是 AWS 受管政策。

使用此政策

您可以將 SystemAdministrator 連接至使用者、群組與角色。

政策詳細資訊

- 類型：任務函數政策
- 建立時間：2016 年 11 月 10 日 17：23 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/job-function/SystemAdministrator

政策版本

政策版本： v12 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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:GetSecurityGroupsForVpc",
        "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",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:PutNotificationSettings",
        "rolesanywhere:ResetNotificationSettings",
        "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"
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

TranslateFullAccess

描述：提供 Amazon Translate 的完整存取權。

`TranslateFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `TranslateFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 27 日，UTC 23：36
- 編輯時間：2020 年 1 月 8 日 21：22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

TranslateReadOnly

描述：提供 Amazon Translate 的唯讀存取權。

`TranslateReadOnly` 是 AWS 受管政策。

使用此政策

您可以將 `TranslateReadOnly` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2017 年 11 月 29 日 18：22 UTC
- 編輯時間：2023 年 5 月 24 日 17：19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

政策版本

政策版本： v7 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

ViewOnlyAccess

描述：此政策授予許可，以檢視所有 AWS 服務的資源和基本中繼資料。

`ViewOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 ViewOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型：任務函數政策
- 建立時間：2016 年 11 月 10 日 17：20 UTC
- 編輯時間：2026 年 2 月 12 日 18：02 UTC
- ARN: arn:aws:iam::aws:policy/job-function/ViewOnlyAccess

政策版本

政策版本： v43 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationGroup",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "backup:DescribeBackupJob",
        "backup:DescribeBackupVault",
        "backup:DescribeCopyJob",
        "backup:DescribeFramework",
```

```
            "backup:DescribeGlobalSettings",
            "backup:DescribeProtectedResource",
            "backup:DescribeRecoveryPoint",
            "backup:DescribeRegionSettings",
            "backup:DescribeReportJob",
            "backup:DescribeReportPlan",
            "backup:DescribeRestoreJob",
            "backup:GetSupportedResourceTypes",
            "backup:ListBackupJobs",
            "backup:ListBackupPlans",
            "backup:ListBackupPlanTemplates",
            "backup:ListBackupPlanVersions",
            "backup:ListBackupSelections",
            "backup:ListBackupVaults",
            "backup:ListCopyJobs",
            "backup:ListFrameworks",
            "backup:ListLegalHolds",
            "backup:ListProtectedResources",
            "backup:ListProtectedResourcesByBackupVault",
            "backup:ListRecoveryPointsByBackupVault",
            "backup:ListRecoveryPointsByLegalHold",
            "backup:ListRecoveryPointsByResource",
            "backup:ListReportJobs",
            "backup:ListReportPlans",
            "backup:ListRestoreJobs",
            "backup:ListTags",
            "batch:ListJobs",
            "bedrock:ListCustomModels",
            "bedrock:ListTagsForResource",
            "clouddirectory:ListAppliedSchemaArns",
            "clouddirectory:ListDevelopmentSchemaArns",
            "clouddirectory:ListDirectories",
            "clouddirectory:ListPublishedSchemaArns",
            "cloudformation:DescribeStacks",
            "cloudformation:List*",
            "cloudfront:List*",
            "cloudsearch:DescribeDomains",
            "cloudsearch:List*",
            "cloudtrail:DescribeTrails",
            "cloudtrail:ListTrails",
            "cloudtrail:LookupEvents",
            "cloudwatch:Get*",
            "cloudwatch:List*",
            "codebuild:ListBuilds*",
```

```
            "codebuild:ListProjects",
            "codecommit:List*",
            "codedeploy:BatchGetApplicationRevisions",
            "codedeploy:BatchGetApplications",
            "codedeploy:BatchGetDeploymentGroups",
            "codedeploy:BatchGetDeploymentInstances",
            "codedeploy:BatchGetDeployments",
            "codedeploy:BatchGetDeploymentTargets",
            "codedeploy:BatchGetOnPremisesInstances",
            "codedeploy:Get*",
            "codedeploy:List*",
            "codepipeline:ListPipelines",
            "codestar:List*",
            "cognito-identity:ListIdentities",
            "cognito-identity:ListIdentityPools",
            "cognito-idp:List*",
            "cognito-sync:ListDatasets",
            "comprehend:Describe*",
            "comprehend:List*",
            "config:Describe*",
            "config:List*",
            "connect:List*",
            "cost-optimization-hub:GetPreferences",
            "cost-optimization-hub:GetRecommendation",
            "cost-optimization-hub:ListEnrollmentStatuses",
            "cost-optimization-hub:ListRecommendations",
            "cost-optimization-hub:ListRecommendationSummaries",
            "databrew:ListJobs",
            "databrew:ListProjects",
            "datapipeline:DescribePipelines",
            "datapipeline:GetAccountLimits",
            "datapipeline:ListPipelines",
            "dax:DescribeClusters",
            "dax:DescribeDefaultParameters",
            "dax:DescribeEvents",
            "dax:DescribeParameterGroups",
            "dax:DescribeParameters",
            "dax:DescribeSubnetGroups",
            "dax:ListTags",
            "devicefarm:List*",
            "directconnect:Describe*",
            "discovery:List*",
            "dms:List*",
            "ds:DescribeDirectories",
```

```
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHost*",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetwork*",
```

```
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnGateways",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "eks:ListTagsForResource",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "emr-serverless:ListApplications",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
```

```
        "fsx:DescribeFileSystems",
        "gamelift:List*",
        "glacier:List*",
        "glue:GetTags",
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
        "inspector:List*",
        "iot:List*",
        "kafka:ListClusters",
        "kendra:ListDataSources",
        "kendra:ListTagsForResource",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lambda:List*",
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBots",
        "lex:GetBotVersions",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "logs:GetTransformer",
        "logs:ListEntitiesForLogGroup",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs",
```

```
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListRouterInputs",
        "mediaconnect:ListRouterOutputs",
        "mediaconnect:ListRouterNetworkInterfaces",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetImportJobs",
        "mobiletargeting:GetSegments",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "opsworks-cm:Describe*",
        "opsworks:Describe*",
        "organizations:List*",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites",
        "outposts:ListTagsForResource",
        "polly:Describe*",
        "polly:List*",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "rds:Describe*",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEvents",
        "redshift:ViewQueriesInConsole",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
```

```
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
        "ses:DescribeActiveReceiptRuleSet",
        "ses:List*",
        "ses:ListDedicatedIpPools",
        "shield:List*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListExecutions",
        "states:ListMapRuns",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
```

```
        "states:ListStateMachineVersions",
        "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*",
        "xray:GetEncryptionConfig",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries",
        "xray:GetSamplingTargets",
        "xray:GetTraceSegmentDestination",
        "xray:ListResourcePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Sid" : "APIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
```

```
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

VMImportExportRoleForAWSConnector

描述：VM Import/Export 服務角色的預設政策，適用於使用 AWS Connector 的客戶。VM Import/Export 服務會擔任此政策的角色，以滿足 AWS 連接器虛擬設備的虛擬機器遷移請求。（請注意，AWS Connector 使用「AWSConnector」受管政策，代表客戶向 VM Import/Export 服務發出請求。）提供建立 AMIs 和 EBS 快照、修改 EBS 快照屬性、對 EC2 物件進行 "Describe*" 呼叫，以及從 'import-to-ec2-' 開始讀取 S3 儲存貯體的功能。

`VMImportExportRoleForAWSConnector` 是 AWS 受管政策。

使用此政策

您可以將 `VMImportExportRoleForAWSConnector` 連接至使用者、群組與角色。

政策詳細資訊

- 類型：服務角色政策
- 建立時間：2015 年 9 月 3 日 20：48 UTC
- 編輯時間：2015 年 9 月 3 日 20：48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

VPCLatticeFullAccess

描述：提供 Amazon VPC Lattice 的完整存取權和相依性服務的存取權。

`VPCLatticeFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `VPCLatticeFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 3 月 30 日 02：49 UTC

- **編輯時間**：2026 年 2 月 12 日 17：57 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "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"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

VPCLatticeReadOnlyAccess

描述：透過 提供對 Amazon VPC Lattice 的唯讀存取權 AWS 管理主控台，以及對相依性服務的有限存取權。

VPCLatticeReadOnlyAccess 是 AWS 受管政策。

使用此政策

您可以將 VPCLatticeReadOnlyAccess 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2023 年 3 月 30 日 02：47 UTC
- 編輯時間：2026 年 2 月 12 日 17：58 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess

政策版本

政策版本： v4 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

VPCLatticeServicesInvokeAccess

描述：提供叫用 Amazon VPC Lattice 服務的存取權。

VPCLatticeServicesInvokeAccess 是 AWS 受管政策。

使用此政策

您可以將 VPCLatticeServicesInvokeAccess 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2023 年 3 月 30 日 02：45 UTC
- 編輯時間：2023 年 3 月 30 日 02：45 UTC
- ARN: arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

WAFLoggingServiceRolePolicy

描述：建立 SLR 以將客戶的日誌寫入 Firehose 串流

`WAFLoggingServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 8 月 24 日，UTC 21：05
- 編輯時間：2018 年 8 月 24 日，UTC 21：05
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

WAFRegionalLoggingServiceRolePolicy

描述：建立 SLR 以將客戶的日誌寫入 Firehose 串流

`WAFRegionalLoggingServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，允許服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2018 年 8 月 24 日 18：40 UTC
- 編輯時間：2018 年 8 月 24 日 18：40 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進

WAFV2LoggingServiceRolePolicy

描述：此政策會建立服務連結角色，允許 AWS WAF 將日誌寫入 Amazon Kinesis Data Firehose。

`WAFV2LoggingServiceRolePolicy` 是 AWS 受管政策。

使用此政策

此政策會連接到服務連結角色，讓服務代表您執行動作。您無法將此政策連接至使用者、群組或角色。

政策詳細資訊

- 類型：服務連結角色政策
- 建立時間：2019 年 11 月 7 日 00：40 UTC
- 編輯時間：2024 年 6 月 3 日 17：29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

政策版本

政策版本： v3 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FirehoseAPIStatement",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "DescribeOrganizationAPIStatement",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
```

```
    }
  ]
}
```

進一步了解

- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

WellArchitectedConsoleFullAccess

描述：透過 提供 AWS Well-Architected Tool 的完整存取權 AWS 管理主控台

`WellArchitectedConsoleFullAccess` 是 AWS 受管政策。

使用此政策

您可以將 `WellArchitectedConsoleFullAccess` 連接至使用者、群組與角色。

政策詳細資訊

- 類型： AWS 受管政策
- 建立時間：2018 年 11 月 29 日 18：19 UTC
- 編輯時間：2018 年 11 月 29 日 18：19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策，並邁向最低權限許可

WellArchitectedConsoleReadOnlyAccess

描述：透過 提供對 AWS Well-Architected Tool 的唯讀存取權 AWS 管理主控台

`WellArchitectedConsoleReadOnlyAccess` 是 AWS 受管政策。

使用此政策

您可以將 `WellArchitectedConsoleReadOnlyAccess` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策
- 建立時間：2018 年 11 月 29 日 18：21 UTC
- 編輯時間：2023 年 6 月 29 日 17：16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

政策版本

政策版本： v2 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集
- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

WorkLinkServiceRolePolicy

描述：允許存取 Amazon WorkLink 使用或管理的 AWS 服務 和 資源

`WorkLinkServiceRolePolicy` 是 AWS 受管政策。

使用此政策

您可以將 `WorkLinkServiceRolePolicy` 連接至使用者、群組與角色。

政策詳細資訊

- Type： AWS 受管政策

- 建立時間：2019 年 1 月 23 日 19：03 UTC
- 編輯時間：2019 年 1 月 23 日 19：03 UTC
- ARN: arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy

政策版本

政策版本： v1 （預設）

政策的預設版本是定義政策許可的版本。當具有 政策的使用者或角色提出存取 AWS 資源的請求時，會 AWS 檢查政策的預設版本，以決定是否允許請求。

JSON 政策文件

```
{
  "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-*"
    }
  ]
}
```

進一步了解

- 在 IAM Identity Center 中使用 AWS 受管政策建立許可集

- 新增和移除 IAM 身分許可
- 了解 IAM 政策的版本控制
- 開始使用 AWS 受管政策並邁向最低權限許可

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。