Referenzhandbuch

AWS Verwaltete Richtlinie

AWS Verwaltete Richtlinie: Referenzhandbuch

Table of Contents

Was sind -AWSverwaltete Richtlinien? 1
Grundlegendes zu Richtlinienreferenzseiten 1
Veraltete, von AWS verwaltete Richtlinien 2
AWS verwaltete Richtlinien 3
AccessAnalyzerServiceRolePolicy 44
Diese Richtlinie wird verwendet 44
Einzelheiten der Richtlinie 44
Version der Richtlinie 44
JSON-Richtliniendokument 45
Weitere Informationen 47
AdministratorAccess 47
Diese Richtlinie wird verwendet 47
Einzelheiten zu den Richtlinien 47
Version der Richtlinie 48
JSON-Richtliniendokument 48
Weitere Informationen 48
AdministratorAccess-Amplify 48
Diese Richtlinie wird verwendet 49
Einzelheiten zu den Richtlinien 49
Version der Richtlinie 49
JSON-Richtliniendokument 49
Weitere Informationen 59
AdministratorAccess-AWSElasticBeanstalk 60
Diese Richtlinie wird verwendet 60
Einzelheiten zu den Richtlinien 60
Version der Richtlinie 60
JSON-Richtliniendokument 60
Weitere Informationen 69
AlexaForBusinessDeviceSetup 69
Diese Richtlinie wird verwendet 69
Einzelheiten zu den Richtlinien 69
Version der Richtlinie 69
JSON-Richtliniendokument 70
Weitere Informationen 70

AlexaForBusinessFullAccess 71
Diese Richtlinie wird verwendet 71
Einzelheiten zu den Richtlinien 71
Version der Richtlinie 71
JSON-Richtliniendokument 71
Weitere Informationen 73
AlexaForBusinessGatewayExecution 73
Diese Richtlinie wird verwendet 73
Einzelheiten zu den Richtlinien 73
Version der Richtlinie 73
JSON-Richtliniendokument 74
Weitere Informationen 74
AlexaForBusinessLifesizeDelegatedAccessPolicy 75
Diese Richtlinie wird verwendet 75
Einzelheiten zu den Richtlinien 75
Version der Richtlinie 75
JSON-Richtliniendokument 75
Weitere Informationen 78
AlexaForBusinessNetworkProfileServicePolicy 78
Diese Richtlinie wird verwendet 78
Einzelheiten der Richtlinie 78
Version der Richtlinie 78
JSON-Richtliniendokument 79
Weitere Informationen 79
AlexaForBusinessPolyDelegatedAccessPolicy 80
Diese Richtlinie wird verwendet 80
Einzelheiten zu den Richtlinien 80
Version der Richtlinie 80
JSON-Richtliniendokument 80
Weitere Informationen 82
AlexaForBusinessReadOnlyAccess 82
Diese Richtlinie wird verwendet 82
Einzelheiten zu den Richtlinien 82
Version der Richtlinie 83
JSON-Richtliniendokument 83
Weitere Informationen 83

AmazonAPIGatewayAdministrator 84
Diese Richtlinie wird verwendet 84
Einzelheiten zu den Richtlinien 84
Version der Richtlinie 84
JSON-Richtliniendokument 84
Weitere Informationen 85
AmazonAPIGatewayInvokeFullAccess 85
Diese Richtlinie wird verwendet 85
Einzelheiten zu den Richtlinien 85
Version der Richtlinie 85
JSON-Richtliniendokument 86
Weitere Informationen 86
AmazonAPIGatewayPushToCloudWatchLogs 86
Diese Richtlinie wird verwendet 86
Einzelheiten zu den Richtlinien 86
Version der Richtlinie 87
JSON-Richtliniendokument 87
Weitere Informationen 87
AmazonAppFlowFullAccess 88
Diese Richtlinie wird verwendet 88
Einzelheiten zu den Richtlinien 88
Version der Richtlinie 88
JSON-Richtliniendokument 88
Weitere Informationen 91
AmazonAppFlowReadOnlyAccess 91
Diese Richtlinie wird verwendet 92
Einzelheiten zu den Richtlinien 92
Version der Richtlinie 92
JSON-Richtliniendokument 92
Weitere Informationen 93
AmazonAppStreamFullAccess 93
Diese Richtlinie wird verwendet 93
Einzelheiten zu den Richtlinien 93
Version der Richtlinie 93
JSON-Richtliniendokument 94
Weitere Informationen 95

AmazonAppStreamPCAAccess 96
Diese Richtlinie wird verwendet 96
Einzelheiten zu den Richtlinien 96
Version der Richtlinie 96
JSON-Richtliniendokument 96
Weitere Informationen 97
AmazonAppStreamReadOnlyAccess 97
Diese Richtlinie wird verwendet 97
Einzelheiten zu den Richtlinien 97
Version der Richtlinie 98
JSON-Richtliniendokument 98
Weitere Informationen 98
AmazonAppStreamServiceAccess 99
Diese Richtlinie wird verwendet 99
Einzelheiten zu den Richtlinien 99
Version der Richtlinie 99
JSON-Richtliniendokument 99
Weitere Informationen 100
AmazonAthenaFullAccess 101
Diese Richtlinie wird verwendet 101
Einzelheiten zu den Richtlinien 101
Version der Richtlinie 101
JSON-Richtliniendokument 101
Weitere Informationen 105
AmazonAugmentedAIFullAccess 105
Diese Richtlinie wird verwendet 105
Einzelheiten zu den Richtlinien 105
Version der Richtlinie 105
JSON-Richtliniendokument 106
Weitere Informationen 107
AmazonAugmentedAIHumanLoopFullAccess 107
Diese Richtlinie wird verwendet 107
Einzelheiten zu den Richtlinien 107
Version der Richtlinie 107
JSON-Richtliniendokument 108
Weitere Informationen 108

AmazonAugmentedAIIntegratedAPIAccess 108
Diese Richtlinie wird verwendet 108
Einzelheiten zu den Richtlinien 109
Version der Richtlinie 109
JSON-Richtliniendokument 109
Weitere Informationen 110
AmazonBedrockFullAccess 111
Diese Richtlinie wird verwendet 111
Einzelheiten zu den Richtlinien 111
Version der Richtlinie 111
JSON-Richtliniendokument 111
Weitere Informationen 112
AmazonBedrockReadOnly 113
Diese Richtlinie wird verwendet 113
Einzelheiten zu den Richtlinien 113
Version der Richtlinie 113
JSON-Richtliniendokument 113
Weitere Informationen 114
AmazonBraketFullAccess 114
Diese Richtlinie wird verwendet 114
Einzelheiten zu den Richtlinien 115
Version der Richtlinie 115
JSON-Richtliniendokument 115
Weitere Informationen 119
AmazonBraketJobsExecutionPolicy 119
Diese Richtlinie wird verwendet 119
Einzelheiten zu den Richtlinien 120
Version der Richtlinie 120
JSON-Richtliniendokument 120
Weitere Informationen 122
AmazonBraketServiceRolePolicy 123
Diese Richtlinie wird verwendet 123
Einzelheiten der Richtlinie 123
Version der Richtlinie 123
JSON-Richtliniendokument 124
Weitere Informationen 124

AmazonChimeFullAccess 124
Diese Richtlinie wird verwendet 125
Einzelheiten zu den Richtlinien 125
Version der Richtlinie 125
JSON-Richtliniendokument 125
Weitere Informationen 127
AmazonChimeReadOnly 127
Diese Richtlinie wird verwendet 128
Einzelheiten zu den Richtlinien 128
Version der Richtlinie 128
JSON-Richtliniendokument 128
Weitere Informationen 129
AmazonChimeSDK 129
Diese Richtlinie wird verwendet 129
Einzelheiten zu den Richtlinien 129
Version der Richtlinie 129
JSON-Richtliniendokument 129
Weitere Informationen 131
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 131
Diese Richtlinie wird verwendet 131
Einzelheiten der Richtlinie 131
Version der Richtlinie 131
JSON-Richtliniendokument 132
Weitere Informationen 133
AmazonChimeSDKMessagingServiceRolePolicy 133
Diese Richtlinie wird verwendet 133
Einzelheiten der Richtlinie 133
Version der Richtlinie 134
JSON-Richtliniendokument 134
Weitere Informationen 135
AmazonChimeServiceRolePolicy 135
Diese Richtlinie wird verwendet 135
Einzelheiten der Richtlinie 135
Version der Richtlinie 135
JSON-Richtliniendokument 136
Weitere Informationen 136

AmazonChimeTranscriptionServiceLinkedRolePolicy 136
Diese Richtlinie wird verwendet 137
Einzelheiten der Richtlinie 137
Version der Richtlinie 137
JSON-Richtliniendokument 137
Weitere Informationen 138
AmazonChimeUserManagement 138
Diese Richtlinie wird verwendet 138
Einzelheiten zu den Richtlinien 138
Version der Richtlinie 138
JSON-Richtliniendokument 138
Weitere Informationen 140
AmazonChimeVoiceConnectorServiceLinkedRolePolicy 140
Diese Richtlinie wird verwendet 140
Einzelheiten der Richtlinie 140
Version der Richtlinie 140
JSON-Richtliniendokument 141
Weitere Informationen 142
AmazonCloudDirectoryFullAccess 143
Diese Richtlinie wird verwendet 143
Einzelheiten zu den Richtlinien 143
Version der Richtlinie 143
JSON-Richtliniendokument 143
Weitere Informationen 144
AmazonCloudDirectoryReadOnlyAccess 144
Diese Richtlinie wird verwendet 144
Einzelheiten zu den Richtlinien 144
Version der Richtlinie 144
JSON-Richtliniendokument 145
Weitere Informationen 145
AmazonCloudWatchEvidentlyFullAccess 145
Diese Richtlinie wird verwendet 146
Einzelheiten zu den Richtlinien 146
Version der Richtlinie 146
JSON-Richtliniendokument 146
Weitere Informationen 149

AmazonCloudWatchEvidentlyReadOnlyAccess 149
Diese Richtlinie wird verwendet 149
Einzelheiten zu den Richtlinien 149
Version der Richtlinie 149
JSON-Richtliniendokument 150
Weitere Informationen 150
AmazonCloudWatchEvidentlyServiceRolePolicy 150
Diese Richtlinie wird verwendet 151
Einzelheiten der Richtlinie 151
Version der Richtlinie 151
JSON-Richtliniendokument 151
Weitere Informationen 153
AmazonCloudWatchRUMFullAccess 153
Diese Richtlinie wird verwendet 153
Einzelheiten zu den Richtlinien 153
Version der Richtlinie 153
JSON-Richtliniendokument 153
Weitere Informationen 156
AmazonCloudWatchRUMReadOnlyAccess 156
Diese Richtlinie wird verwendet 156
Einzelheiten zu den Richtlinien 156
Version der Richtlinie 157
JSON-Richtliniendokument 157
Weitere Informationen 157
AmazonCloudWatchRUMServiceRolePolicy 158
Diese Richtlinie wird verwendet 158
Einzelheiten der Richtlinie 158
Version der Richtlinie 158
JSON-Richtliniendokument 158
Weitere Informationen 159
AmazonCodeCatalystFullAccess 159
Diese Richtlinie wird verwendet 159
Einzelheiten zu den Richtlinien 159
Version der Richtlinie 160
JSON-Richtliniendokument 160
Weitere Informationen 161

AmazonCodeCatalystReadOnlyAccess 161
Diese Richtlinie wird verwendet 161
Einzelheiten zu den Richtlinien 161
Version der Richtlinie 161
JSON-Richtliniendokument 162
Weitere Informationen 162
AmazonCodeCatalystSupportAccess 162
Diese Richtlinie wird verwendet 162
Einzelheiten zu den Richtlinien 163
Version der Richtlinie 163
JSON-Richtliniendokument 163
Weitere Informationen 164
AmazonCodeGuruProfilerAgentAccess 164
Diese Richtlinie wird verwendet 164
Einzelheiten zu den Richtlinien 164
Version der Richtlinie 164
JSON-Richtliniendokument 165
Weitere Informationen 165
AmazonCodeGuruProfilerFullAccess 165
Diese Richtlinie wird verwendet 166
Einzelheiten zu den Richtlinien 166
Version der Richtlinie 166
JSON-Richtliniendokument 166
Weitere Informationen 167
AmazonCodeGuruProfilerReadOnlyAccess 167
Diese Richtlinie wird verwendet 167
Einzelheiten zu den Richtlinien 167
Version der Richtlinie 168
JSON-Richtliniendokument 168
Weitere Informationen 168
AmazonCodeGuruReviewerFullAccess 169
Diese Richtlinie wird verwendet 169
Einzelheiten zu den Richtlinien 169
Version der Richtlinie 169
JSON-Richtliniendokument 169
Weitere Informationen 172

AmazonCodeGuruReviewerReadOnlyAccess 172
Diese Richtlinie wird verwendet 172
Einzelheiten zu den Richtlinien 172
Version der Richtlinie 173
JSON-Richtliniendokument 173
Weitere Informationen 173
AmazonCodeGuruReviewerServiceRolePolicy 174
Diese Richtlinie wird verwendet 174
Einzelheiten der Richtlinie 174
Version der Richtlinie 174
JSON-Richtliniendokument 174
Weitere Informationen 176
AmazonCodeGuruSecurityFullAccess 176
Diese Richtlinie wird verwendet 177
Einzelheiten zu den Richtlinien 177
Version der Richtlinie 177
JSON-Richtliniendokument 177
Weitere Informationen 178
AmazonCodeGuruSecurityScanAccess 178
Diese Richtlinie wird verwendet 178
Einzelheiten zu den Richtlinien 178
Version der Richtlinie 178
JSON-Richtliniendokument 179
Weitere Informationen 179
AmazonCognitoDeveloperAuthenticatedIdentities 179
Diese Richtlinie wird verwendet 179
Einzelheiten zu den Richtlinien 180
Version der Richtlinie 180
JSON-Richtliniendokument 180
Weitere Informationen 180
AmazonCognitoIdpEmailServiceRolePolicy 181
Diese Richtlinie wird verwendet 181
Einzelheiten der Richtlinie 181
Version der Richtlinie 181
JSON-Richtliniendokument 181
Weitere Informationen 182

AmazonCognitoIdpServiceRolePolicy 182
Diese Richtlinie wird verwendet 182
Einzelheiten der Richtlinie 183
Version der Richtlinie 183
JSON-Richtliniendokument 183
Weitere Informationen 183
AmazonCognitoPowerUser 184
Diese Richtlinie wird verwendet 184
Einzelheiten zu den Richtlinien 184
Version der Richtlinie 184
JSON-Richtliniendokument 184
Weitere Informationen 186
AmazonCognitoReadOnly 186
Diese Richtlinie wird verwendet 186
Einzelheiten zu den Richtlinien 186
Version der Richtlinie 186
JSON-Richtliniendokument 187
Weitere Informationen 187
AmazonCognitoUnAuthedIdentitiesSessionPolicy 188
Diese Richtlinie wird verwendet 188
Einzelheiten zu den Richtlinien 188
Version der Richtlinie 188
JSON-Richtliniendokument 189
Weitere Informationen 189
AmazonCognitoUnauthenticatedIdentities 189
Diese Richtlinie wird verwendet 190
Einzelheiten zu den Richtlinien 190
Version der Richtlinie 190
JSON-Richtliniendokument 190
Weitere Informationen 191
AmazonConnect_FullAccess 191
Diese Richtlinie wird verwendet 191
Einzelheiten zu den Richtlinien 191
Version der Richtlinie 191
JSON-Richtliniendokument 192
Weitere Informationen 194

AmazonConnectCampaignsServiceLinkedRolePolicy 194
Diese Richtlinie wird verwendet 195
Einzelheiten der Richtlinie 195
Version der Richtlinie 195
JSON-Richtliniendokument 195
Weitere Informationen 196
AmazonConnectReadOnlyAccess 196
Diese Richtlinie wird verwendet 196
Einzelheiten zu den Richtlinien 196
Version der Richtlinie 196
JSON-Richtliniendokument 197
Weitere Informationen 197
AmazonConnectServiceLinkedRolePolicy 197
Diese Richtlinie wird verwendet 198
Einzelheiten der Richtlinie 198
Version der Richtlinie 198
JSON-Richtliniendokument 198
Weitere Informationen 203
AmazonConnectSynchronizationServiceRolePolicy 204
Diese Richtlinie wird verwendet 204
Einzelheiten der Richtlinie 204
Version der Richtlinie 204
JSON-Richtliniendokument 204
Weitere Informationen 206
AmazonConnectVoiceIDFullAccess 207
Diese Richtlinie wird verwendet 207
Einzelheiten zu den Richtlinien 207
Version der Richtlinie 207
JSON-Richtliniendokument 207
Weitere Informationen 208
AmazonDataZoneDomainExecutionRolePolicy 208
Diese Richtlinie wird verwendet 208
Einzelheiten zu den Richtlinien 208
Version der Richtlinie 208
JSON-Richtliniendokument 209
Weitere Informationen 211

AmazonDataZoneEnvironmentRolePermissionsBoundary 212
Diese Richtlinie wird verwendet 212
Einzelheiten zu den Richtlinien 212
Version der Richtlinie 212
JSON-Richtliniendokument 212
Weitere Informationen 225
AmazonDataZoneFullAccess 225
Diese Richtlinie wird verwendet 226
Einzelheiten zu den Richtlinien 226
Version der Richtlinie 226
JSON-Richtliniendokument 226
Weitere Informationen 230
AmazonDataZoneFullUserAccess 230
Diese Richtlinie wird verwendet 230
Einzelheiten zu den Richtlinien 230
Version der Richtlinie 230
JSON-Richtliniendokument 231
Weitere Informationen 233
AmazonDataZoneGlueManageAccessRolePolicy 234
Diese Richtlinie wird verwendet 234
Einzelheiten zu den Richtlinien 234
Version der Richtlinie 234
JSON-Richtliniendokument 234
Weitere Informationen 239
AmazonDataZonePortalFullAccessPolicy 240
Diese Richtlinie wird verwendet 240
Einzelheiten zu den Richtlinien 240
Version der Richtlinie 240
JSON-Richtliniendokument 240
Weitere Informationen 241
AmazonDataZonePreviewConsoleFullAccess 241
Diese Richtlinie wird verwendet 241
Einzelheiten zu den Richtlinien 241
Version der Richtlinie 241
JSON-Richtliniendokument 242
Weitere Informationen 243

AmazonDataZoneProjectDeploymentPermissionsBoundary 244
Diese Richtlinie wird verwendet 244
Einzelheiten zu den Richtlinien 244
Version der Richtlinie 244
JSON-Richtliniendokument 245
Weitere Informationen 253
AmazonDataZoneProjectRolePermissionsBoundary 253
Diese Richtlinie wird verwendet 253
Einzelheiten zu den Richtlinien 253
Version der Richtlinie 253
JSON-Richtliniendokument 254
Weitere Informationen 261
AmazonDataZoneRedshiftGlueProvisioningPolicy 261
Diese Richtlinie wird verwendet 261
Einzelheiten zu den Richtlinien 261
Version der Richtlinie 262
JSON-Richtliniendokument 262
Weitere Informationen 269
AmazonDataZoneRedshiftManageAccessRolePolicy 270
Diese Richtlinie wird verwendet 270
Einzelheiten zu den Richtlinien 270
Version der Richtlinie 270
JSON-Richtliniendokument 270
Weitere Informationen 273
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 273
Diese Richtlinie wird verwendet 273
Einzelheiten zu den Richtlinien 273
Version der Richtlinie 273
JSON-Richtliniendokument 274
Weitere Informationen 301
AmazonDataZoneSageMakerManageAccessRolePolicy 301
Diese Richtlinie wird verwendet 301
Einzelheiten zu den Richtlinien 301
Version der Richtlinie 302
JSON-Richtliniendokument 302
Weitere Informationen 306

AmazonDataZoneSageMakerProvisioningRolePolicy 307
Diese Richtlinie wird verwendet 307
Einzelheiten zu den Richtlinien 307
Version der Richtlinie 307
JSON-Richtliniendokument 307
Weitere Informationen 312
AmazonDetectiveFullAccess 312
Diese Richtlinie wird verwendet 312
Einzelheiten zu den Richtlinien 313
Version der Richtlinie 313
JSON-Richtliniendokument 313
Weitere Informationen 314
AmazonDetectiveInvestigatorAccess 314
Diese Richtlinie wird verwendet 314
Einzelheiten zu den Richtlinien 315
Version der Richtlinie 315
JSON-Richtliniendokument 315
Weitere Informationen 316
AmazonDetectiveMemberAccess 317
Diese Richtlinie wird verwendet 317
Einzelheiten zu den Richtlinien 317
Version der Richtlinie 317
JSON-Richtliniendokument 317
Weitere Informationen 318
AmazonDetectiveOrganizationsAccess 318
Diese Richtlinie wird verwendet 318
Einzelheiten zu den Richtlinien 319
Version der Richtlinie 319
JSON-Richtliniendokument 319
Weitere Informationen 321
AmazonDetectiveServiceLinkedRolePolicy 321
Diese Richtlinie wird verwendet 321
Einzelheiten der Richtlinie 321
Version der Richtlinie 321
JSON-Richtliniendokument 322
Weitere Informationen 322

AmazonDevOpsGuruConsoleFullAccess 322
Diese Richtlinie wird verwendet 322
Einzelheiten zu den Richtlinien 322
Version der Richtlinie 323
JSON-Richtliniendokument 323
Weitere Informationen 325
AmazonDevOpsGuruFullAccess 326
Diese Richtlinie wird verwendet 326
Einzelheiten zu den Richtlinien 326
Version der Richtlinie 326
JSON-Richtliniendokument 326
Weitere Informationen 328
AmazonDevOpsGuruOrganizationsAccess 329
Diese Richtlinie wird verwendet 329
Einzelheiten zu den Richtlinien 329
Version der Richtlinie 329
JSON-Richtliniendokument 329
Weitere Informationen 331
AmazonDevOpsGuruReadOnlyAccess 331
Diese Richtlinie wird verwendet 331
Einzelheiten zu den Richtlinien 331
Version der Richtlinie 331
JSON-Richtliniendokument 332
Weitere Informationen 333
AmazonDevOpsGuruServiceRolePolicy 334
Diese Richtlinie wird verwendet 334
Einzelheiten der Richtlinie 334
Version der Richtlinie 334
JSON-Richtliniendokument 335
Weitere Informationen 339
AmazonDMSCloudWatchLogsRole 339
Diese Richtlinie wird verwendet 339
Einzelheiten zu den Richtlinien 339
Version der Richtlinie 339
JSON-Richtliniendokument 339
Weitere Informationen 341

AmazonDMSRedshiftS3Role ... 341
Diese Richtlinie wird verwendet ... 341
Einzelheiten zu den Richtlinien ... 341
Version der Richtlinie ... 342
JSON-Richtliniendokument ... 342
Weitere Informationen ... 343
AmazonDMSVPCManagementRole ... 343
Diese Richtlinie wird verwendet ... 343
Einzelheiten zu den Richtlinien ... 343
Version der Richtlinie ... 343
JSON-Richtliniendokument ... 344
Weitere Informationen ... 344
AmazonDocDB-ElasticServiceRolePolicy ... 344
Diese Richtlinie wird verwendet ... 345
Einzelheiten der Richtlinie ... 345
Version der Richtlinie ... 345
JSON-Richtliniendokument ... 345
Weitere Informationen ... 346
AmazonDocDBConsoleFullAccess ... 346
Diese Richtlinie wird verwendet ... 346
Einzelheiten zu den Richtlinien ... 346
Version der Richtlinie ... 347
JSON-Richtliniendokument ... 347
Weitere Informationen ... 351
AmazonDocDBElasticFullAccess ... 351
Diese Richtlinie wird verwendet ... 351
Einzelheiten zu den Richtlinien ... 351
Version der Richtlinie ... 352
JSON-Richtliniendokument ... 352
Weitere Informationen ... 355
AmazonDocDBElasticReadOnlyAccess ... 355
Diese Richtlinie wird verwendet ... 355
Einzelheiten zu den Richtlinien ... 355
Version der Richtlinie ... 356
JSON-Richtliniendokument ... 356
Weitere Informationen ... 356

AmazonDocDBFullAccess 357
Diese Richtlinie wird verwendet 357
Einzelheiten zu den Richtlinien 357
Version der Richtlinie 357
JSON-Richtliniendokument 357
Weitere Informationen 360
AmazonDocDBReadOnlyAccess 360
Diese Richtlinie wird verwendet 361
Einzelheiten zu den Richtlinien 361
Version der Richtlinie 361
JSON-Richtliniendokument 361
Weitere Informationen 363
AmazonDRSVPCManagement 363
Diese Richtlinie wird verwendet 363
Einzelheiten zu den Richtlinien 363
Version der Richtlinie 364
JSON-Richtliniendokument 364
Weitere Informationen 364
AmazonDynamoDBFullAccess 365
Diese Richtlinie wird verwendet 365
Einzelheiten zu den Richtlinien 365
Version der Richtlinie 365
JSON-Richtliniendokument 365
Weitere Informationen 368
AmazonDynamoDBFullAccesswithDataPipeline 368
Diese Richtlinie wird verwendet 368
Einzelheiten zu den Richtlinien 369
Version der Richtlinie 369
JSON-Richtliniendokument 369
Weitere Informationen 371
AmazonDynamoDBReadOnlyAccess 371
Diese Richtlinie wird verwendet 371
Einzelheiten zu den Richtlinien 372
Version der Richtlinie 372
JSON-Richtliniendokument 372
Weitere Informationen 374

AmazonEBSCSIDriverPolicy 374
Diese Richtlinie wird verwendet 374
Einzelheiten zu den Richtlinien 374
Version der Richtlinie 374
JSON-Richtliniendokument 375
Weitere Informationen 378
AmazonEC2ContainerRegistryFullAccess 378
Diese Richtlinie wird verwendet 378
Einzelheiten zu den Richtlinien 378
Version der Richtlinie 378
JSON-Richtliniendokument 379
Weitere Informationen 379
AmazonEC2ContainerRegistryPowerUser 380
Diese Richtlinie wird verwendet 380
Einzelheiten zu den Richtlinien 380
Version der Richtlinie 380
JSON-Richtliniendokument 380
Weitere Informationen 381
AmazonEC2ContainerRegistryReadOnly 381
Diese Richtlinie wird verwendet 381
Einzelheiten zu den Richtlinien 382
Version der Richtlinie 382
JSON-Richtliniendokument 382
Weitere Informationen 383
AmazonEC2ContainerServiceAutoscaleRole 383
Diese Richtlinie wird verwendet 383
Einzelheiten zu den Richtlinien 383
Version der Richtlinie 383
JSON-Richtliniendokument 384
Weitere Informationen 384
AmazonEC2ContainerServiceEventsRole 384
Diese Richtlinie wird verwendet 385
Einzelheiten zu den Richtlinien 385
Version der Richtlinie 385
JSON-Richtliniendokument 385
Weitere Informationen 386

AmazonEC2ContainerServiceforEC2Role 386
Diese Richtlinie wird verwendet 387
Einzelheiten zu den Richtlinien 387
Version der Richtlinie 387
JSON-Richtliniendokument 387
Weitere Informationen 388
AmazonEC2ContainerServiceRole 388
Diese Richtlinie wird verwendet 389
Einzelheiten zu den Richtlinien 389
Version der Richtlinie 389
JSON-Richtliniendokument 389
Weitere Informationen 390
AmazonEC2FullAccess 390
Diese Richtlinie wird verwendet 390
Einzelheiten zu den Richtlinien 390
Version der Richtlinie 390
JSON-Richtliniendokument 391
Weitere Informationen 392
AmazonEC2ReadOnlyAccess 392
Diese Richtlinie wird verwendet 392
Einzelheiten zu den Richtlinien 392
Version der Richtlinie 392
JSON-Richtliniendokument 393
Weitere Informationen 393
AmazonEC2RoleforAWSCodeDeploy 394
Diese Richtlinie wird verwendet 394
Einzelheiten zu den Richtlinien 394
Version der Richtlinie 394
JSON-Richtliniendokument 394
Weitere Informationen 395
AmazonEC2RoleforAWSCodeDeployLimited 395
Diese Richtlinie wird verwendet 395
Einzelheiten zu den Richtlinien 395
Version der Richtlinie 396
JSON-Richtliniendokument 396
Weitere Informationen 396

AmazonEC2RoleforDataPipelineRole 397
Diese Richtlinie wird verwendet 397
Einzelheiten zu den Richtlinien 397
Version der Richtlinie 397
JSON-Richtliniendokument 397
Weitere Informationen 398
AmazonEC2RoleforSSM 398
Diese Richtlinie wird verwendet 399
Einzelheiten zu den Richtlinien 399
Version der Richtlinie 399
JSON-Richtliniendokument 399
Weitere Informationen 401
AmazonEC2RolePolicyForLaunchWizard 402
Diese Richtlinie wird verwendet 402
Einzelheiten zu den Richtlinien 402
Version der Richtlinie 402
JSON-Richtliniendokument 402
Weitere Informationen 406
AmazonEC2SpotFleetAutoscaleRole 406
Diese Richtlinie wird verwendet 407
Einzelheiten zu den Richtlinien 407
Version der Richtlinie 407
JSON-Richtliniendokument 407
Weitere Informationen 408
AmazonEC2SpotFleetTaggingRole 408
Diese Richtlinie wird verwendet 408
Einzelheiten zu den Richtlinien 409
Version der Richtlinie 409
JSON-Richtliniendokument 409
Weitere Informationen 410
AmazonECS_FullAccess 411
Diese Richtlinie wird verwendet 411
Einzelheiten zu den Richtlinien 411
Version der Richtlinie 411
JSON-Richtliniendokument 411
Weitere Informationen 417

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 417
Diese Richtlinie wird verwendet 417
Einzelheiten zu den Richtlinien 417
Version der Richtlinie 417
JSON-Richtliniendokument 418
Weitere Informationen 420
AmazonECSInfrastructureRolePolicyForVolumes 420
Diese Richtlinie wird verwendet 420
Einzelheiten zu den Richtlinien 420
Version der Richtlinie 421
JSON-Richtliniendokument 421
Weitere Informationen 423
AmazonECSServiceRolePolicy 423
Diese Richtlinie wird verwendet 423
Einzelheiten der Richtlinie 423
Version der Richtlinie 423
JSON-Richtliniendokument 424
Weitere Informationen 428
AmazonECSTaskExecutionRolePolicy 429
Diese Richtlinie wird verwendet 429
Einzelheiten zu den Richtlinien 429
Version der Richtlinie 429
JSON-Richtliniendokument 429
Weitere Informationen 430
AmazonEFSCSIDriverPolicy 430
Diese Richtlinie wird verwendet 430
Einzelheiten zu den Richtlinien 430
Version der Richtlinie 431
JSON-Richtliniendokument 431
Weitere Informationen 432
AmazonEKS_CNI_Policy 433
Diese Richtlinie wird verwendet 433
Einzelheiten zu den Richtlinien 433
Version der Richtlinie 433
JSON-Richtliniendokument 433
Weitere Informationen 434

AmazonEKSClusterPolicy 435
Diese Richtlinie wird verwendet 435
Einzelheiten zu den Richtlinien 435
Version der Richtlinie 435
JSON-Richtliniendokument 435
Weitere Informationen 437
AmazonEKSConnectorServiceRolePolicy 438
Diese Richtlinie wird verwendet 438
Einzelheiten der Richtlinie 438
Version der Richtlinie 438
JSON-Richtliniendokument 438
Weitere Informationen 440
AmazonEKSFargatePodExecutionRolePolicy 440
Diese Richtlinie wird verwendet 440
Einzelheiten zu den Richtlinien 441
Version der Richtlinie 441
JSON-Richtliniendokument 441
Weitere Informationen 441
AmazonEKSForFargateServiceRolePolicy 442
Diese Richtlinie wird verwendet 442
Einzelheiten der Richtlinie 442
Version der Richtlinie 442
JSON-Richtliniendokument 442
Weitere Informationen 443
AmazonEKSLocalOutpostClusterPolicy 443
Diese Richtlinie wird verwendet 443
Einzelheiten zu den Richtlinien 443
Version der Richtlinie 444
JSON-Richtliniendokument 444
Weitere Informationen 446
AmazonEKSLocalOutpostServiceRolePolicy 446
Diese Richtlinie wird verwendet 446
Einzelheiten der Richtlinie 446
Version der Richtlinie 446
JSON-Richtliniendokument 447
Weitere Informationen 452

AmazonEKSServicePolicy 452
Diese Richtlinie wird verwendet 453
Einzelheiten zu den Richtlinien 453
Version der Richtlinie 453
JSON-Richtliniendokument 453
Weitere Informationen 455
AmazonEKSServiceRolePolicy 455
Diese Richtlinie wird verwendet 455
Einzelheiten der Richtlinie 455
Version der Richtlinie 456
JSON-Richtliniendokument 456
Weitere Informationen 458
AmazonEKSVPCResourceController 458
Diese Richtlinie wird verwendet 458
Einzelheiten zu den Richtlinien 459
Version der Richtlinie 459
JSON-Richtliniendokument 459
Weitere Informationen 460
AmazonEKSWorkerNodePolicy 460
Diese Richtlinie wird verwendet 460
Einzelheiten zu den Richtlinien 460
Version der Richtlinie 460
JSON-Richtliniendokument 461
Weitere Informationen 461
AmazonElastiCacheFullAccess 462
Diese Richtlinie wird verwendet 462
Einzelheiten zu den Richtlinien 462
Version der Richtlinie 462
JSON-Richtliniendokument 462
Weitere Informationen 465
AmazonElastiCacheReadOnlyAccess 466
Diese Richtlinie wird verwendet 466
Einzelheiten zu den Richtlinien 466
Version der Richtlinie 466
JSON-Richtliniendokument 466
Weitere Informationen 467

AmazonElasticContainerRegistryPublicFullAccess 467
Diese Richtlinie wird verwendet 467
Einzelheiten zu den Richtlinien 467
Version der Richtlinie 468
JSON-Richtliniendokument 468
Weitere Informationen 468
AmazonElasticContainerRegistryPublicPowerUser 468
Diese Richtlinie wird verwendet 469
Einzelheiten zu den Richtlinien 469
Version der Richtlinie 469
JSON-Richtliniendokument 469
Weitere Informationen 470
AmazonElasticContainerRegistryPublicReadOnly 470
Diese Richtlinie wird verwendet 470
Einzelheiten zu den Richtlinien 470
Version der Richtlinie 471
JSON-Richtliniendokument 471
Weitere Informationen 471
AmazonElasticFileSystemClientFullAccess 472
Diese Richtlinie wird verwendet 472
Einzelheiten zu den Richtlinien 472
Version der Richtlinie 472
JSON-Richtliniendokument 472
Weitere Informationen 473
AmazonElasticFileSystemClientReadOnlyAccess 473
Diese Richtlinie wird verwendet 473
Einzelheiten zu den Richtlinien 473
Version der Richtlinie 473
JSON-Richtliniendokument 474
Weitere Informationen 474
AmazonElasticFileSystemClientReadWriteAccess 474
Diese Richtlinie wird verwendet 474
Einzelheiten zu den Richtlinien 475
Version der Richtlinie 475
JSON-Richtliniendokument 475
Weitere Informationen 475

AmazonElasticFileSystemFullAccess 476
Diese Richtlinie wird verwendet 476
Einzelheiten zu den Richtlinien 476
Version der Richtlinie 476
JSON-Richtliniendokument 476
Weitere Informationen 478
AmazonElasticFileSystemReadOnlyAccess 478
Diese Richtlinie wird verwendet 479
Einzelheiten zu den Richtlinien 479
Version der Richtlinie 479
JSON-Richtliniendokument 479
Weitere Informationen 480
AmazonElasticFileSystemServiceRolePolicy 480
Diese Richtlinie wird verwendet 480
Einzelheiten der Richtlinie 480
Version der Richtlinie 481
JSON-Richtliniendokument 481
Weitere Informationen 483
AmazonElasticFileSystemsUtils 483
Diese Richtlinie wird verwendet 483
Einzelheiten zu den Richtlinien 483
Version der Richtlinie 484
JSON-Richtliniendokument 484
Weitere Informationen 486
AmazonElasticMapReduceEditorsRole 486
Diese Richtlinie wird verwendet 486
Einzelheiten zu den Richtlinien 486
Version der Richtlinie 486
JSON-Richtliniendokument 487
Weitere Informationen 488
AmazonElasticMapReduceforAutoScalingRole 488
Diese Richtlinie wird verwendet 488
Einzelheiten zu den Richtlinien 488
Version der Richtlinie 489
JSON-Richtliniendokument 489
Weitere Informationen 489

AmazonElasticMapReduceforEC2Role 489
Diese Richtlinie wird verwendet 490
Einzelheiten zu den Richtlinien 490
Version der Richtlinie 490
JSON-Richtliniendokument 490
Weitere Informationen 492
AmazonElasticMapReduceFullAccess 492
Diese Richtlinie wird verwendet 492
Einzelheiten zu den Richtlinien 492
Version der Richtlinie 492
JSON-Richtliniendokument 493
Weitere Informationen 494
AmazonElasticMapReducePlacementGroupPolicy 494
Diese Richtlinie wird verwendet 495
Einzelheiten zu den Richtlinien 495
Version der Richtlinie 495
JSON-Richtliniendokument 495
Weitere Informationen 496
AmazonElasticMapReduceReadOnlyAccess 496
Diese Richtlinie wird verwendet 496
Einzelheiten zu den Richtlinien 496
Version der Richtlinie 496
JSON-Richtliniendokument 497
Weitere Informationen 497
AmazonElasticMapReduceRole 498
Diese Richtlinie wird verwendet 498
Einzelheiten zu den Richtlinien 498
Version der Richtlinie 498
JSON-Richtliniendokument 498
Weitere Informationen 500
AmazonElasticsearchServiceRolePolicy 501
Diese Richtlinie wird verwendet 501
Einzelheiten der Richtlinie 501
Version der Richtlinie 501
JSON-Richtliniendokument 501
Weitere Informationen 504

AmazonElasticTranscoder_FullAccess 504
Diese Richtlinie wird verwendet 505
Einzelheiten zu den Richtlinien 505
Version der Richtlinie 505
JSON-Richtliniendokument 505
Weitere Informationen 506
AmazonElasticTranscoder_JobsSubmitter 506
Diese Richtlinie wird verwendet 506
Einzelheiten zu den Richtlinien 506
Version der Richtlinie 507
JSON-Richtliniendokument 507
Weitere Informationen 507
AmazonElasticTranscoder_ReadOnlyAccess 508
Diese Richtlinie wird verwendet 508
Einzelheiten zu den Richtlinien 508
Version der Richtlinie 508
JSON-Richtliniendokument 508
Weitere Informationen 509
AmazonElasticTranscoderRole 509
Diese Richtlinie wird verwendet 509
Einzelheiten zu den Richtlinien 509
Version der Richtlinie 510
JSON-Richtliniendokument 510
Weitere Informationen 511
AmazonEMRCleanupPolicy 511
Diese Richtlinie wird verwendet 511
Einzelheiten der Richtlinie 511
Version der Richtlinie 511
JSON-Richtliniendokument 512
Weitere Informationen 512
AmazonEMRContainersServiceRolePolicy 513
Diese Richtlinie wird verwendet 513
Einzelheiten der Richtlinie 513
Version der Richtlinie 513
JSON-Richtliniendokument 513
Weitere Informationen 514

AmazonEMRFullAccessPolicy_v2 515
Diese Richtlinie wird verwendet 515
Einzelheiten zu den Richtlinien 515
Version der Richtlinie 515
JSON-Richtliniendokument 515
Weitere Informationen 519
AmazonEMRReadOnlyAccessPolicy_v2 519
Diese Richtlinie wird verwendet 519
Einzelheiten zu den Richtlinien 519
Version der Richtlinie 519
JSON-Richtliniendokument 520
Weitere Informationen 521
AmazonEMRServerlessServiceRolePolicy 521
Diese Richtlinie wird verwendet 521
Einzelheiten der Richtlinie 521
Version der Richtlinie 521
JSON-Richtliniendokument 522
Weitere Informationen 523
AmazonEMRServicePolicy_v2 523
Diese Richtlinie wird verwendet 523
Einzelheiten zu den Richtlinien 523
Version der Richtlinie 523
JSON-Richtliniendokument 524
Weitere Informationen 531
AmazonESCognitoAccess 531
Diese Richtlinie wird verwendet 532
Einzelheiten zu den Richtlinien 532
Version der Richtlinie 532
JSON-Richtliniendokument 532
Weitere Informationen 533
AmazonESFullAccess 533
Diese Richtlinie wird verwendet 533
Einzelheiten zu den Richtlinien 534
Version der Richtlinie 534
JSON-Richtliniendokument 534
Weitere Informationen 534

AmazonESReadOnlyAccess 535
Diese Richtlinie wird verwendet 535
Einzelheiten zu den Richtlinien 535
Version der Richtlinie 535
JSON-Richtliniendokument 535
Weitere Informationen 536
AmazonEventBridgeApiDestinationsServiceRolePolicy 536
Diese Richtlinie wird verwendet 536
Einzelheiten der Richtlinie 536
Version der Richtlinie 536
JSON-Richtliniendokument 537
Weitere Informationen 537
AmazonEventBridgeFullAccess 537
Diese Richtlinie wird verwendet 538
Einzelheiten zu den Richtlinien 538
Version der Richtlinie 538
JSON-Richtliniendokument 538
Weitere Informationen 540
AmazonEventBridgePipesFullAccess 540
Diese Richtlinie wird verwendet 541
Einzelheiten zu den Richtlinien 541
Version der Richtlinie 541
JSON-Richtliniendokument 541
Weitere Informationen 542
AmazonEventBridgePipesOperatorAccess 542
Diese Richtlinie wird verwendet 542
Einzelheiten zu den Richtlinien 542
Version der Richtlinie 542
JSON-Richtliniendokument 543
Weitere Informationen 543
AmazonEventBridgePipesReadOnlyAccess 543
Diese Richtlinie wird verwendet 544
Einzelheiten zu den Richtlinien 544
Version der Richtlinie 544
JSON-Richtliniendokument 544
Weitere Informationen 545

AmazonEventBridgeReadOnlyAccess 545
Diese Richtlinie wird verwendet 545
Einzelheiten zu den Richtlinien 545
Version der Richtlinie 545
JSON-Richtliniendokument 546
Weitere Informationen 547
AmazonEventBridgeSchedulerFullAccess 547
Diese Richtlinie wird verwendet 547
Einzelheiten zu den Richtlinien 547
Version der Richtlinie 548
JSON-Richtliniendokument 548
Weitere Informationen 548
AmazonEventBridgeSchedulerReadOnlyAccess 549
Diese Richtlinie wird verwendet 549
Einzelheiten zu den Richtlinien 549
Version der Richtlinie 549
JSON-Richtliniendokument 549
Weitere Informationen 550
AmazonEventBridgeSchemasFullAccess 550
Diese Richtlinie wird verwendet 550
Einzelheiten zu den Richtlinien 550
Version der Richtlinie 551
JSON-Richtliniendokument 551
Weitere Informationen 552
AmazonEventBridgeSchemasReadOnlyAccess 552
Diese Richtlinie wird verwendet 552
Einzelheiten zu den Richtlinien 552
Version der Richtlinie 552
JSON-Richtliniendokument 553
Weitere Informationen 553
AmazonEventBridgeSchemasServiceRolePolicy 554
Diese Richtlinie wird verwendet 554
Einzelheiten der Richtlinie 554
Version der Richtlinie 554
JSON-Richtliniendokument 554
Weitere Informationen 555

AmazonFISServiceRolePolicy 555
Diese Richtlinie wird verwendet 555
Einzelheiten der Richtlinie 555
Version der Richtlinie 556
JSON-Richtliniendokument 556
Weitere Informationen 557
AmazonForecastFullAccess 558
Diese Richtlinie wird verwendet 558
Einzelheiten zu den Richtlinien 558
Version der Richtlinie 558
JSON-Richtliniendokument 558
Weitere Informationen 559
AmazonFraudDetectorFullAccessPolicy 559
Diese Richtlinie wird verwendet 559
Einzelheiten zu den Richtlinien 559
Version der Richtlinie 560
JSON-Richtliniendokument 560
Weitere Informationen 561
AmazonFreeRTOSFullAccess 561
Diese Richtlinie wird verwendet 561
Einzelheiten zu den Richtlinien 562
Version der Richtlinie 562
JSON-Richtliniendokument 562
Weitere Informationen 562
AmazonFreeRTOSOTAUpdate 563
Diese Richtlinie wird verwendet 563
Einzelheiten zu den Richtlinien 563
Version der Richtlinie 563
JSON-Richtliniendokument 563
Weitere Informationen 565
AmazonFSxConsoleFullAccess 565
Diese Richtlinie wird verwendet 565
Einzelheiten zu den Richtlinien 565
Version der Richtlinie 565
JSON-Richtliniendokument 566
Weitere Informationen 569

AmazonFSxConsoleReadOnlyAccess 569
Diese Richtlinie wird verwendet 569
Einzelheiten zu den Richtlinien 570
Version der Richtlinie 570
JSON-Richtliniendokument 570
Weitere Informationen 571
AmazonFSxFullAccess 571
Diese Richtlinie wird verwendet 571
Einzelheiten zu den Richtlinien 571
Version der Richtlinie 571
JSON-Richtliniendokument 572
Weitere Informationen 576
AmazonFSxReadOnlyAccess 576
Diese Richtlinie wird verwendet 576
Einzelheiten zu den Richtlinien 576
Version der Richtlinie 576
JSON-Richtliniendokument 577
Weitere Informationen 577
AmazonFSxServiceRolePolicy 577
Diese Richtlinie wird verwendet 577
Einzelheiten der Richtlinie 577
Version der Richtlinie 578
JSON-Richtliniendokument 578
Weitere Informationen 581
AmazonGlacierFullAccess 581
Diese Richtlinie wird verwendet 581
Einzelheiten zu den Richtlinien 581
Version der Richtlinie 581
JSON-Richtliniendokument 581
Weitere Informationen 582
AmazonGlacierReadOnlyAccess 582
Diese Richtlinie wird verwendet 582
Einzelheiten zu den Richtlinien 582
Version der Richtlinie 583
JSON-Richtliniendokument 583
Weitere Informationen 583

AmazonGrafanaAthenaAccess 584
Diese Richtlinie wird verwendet 584
Einzelheiten zu den Richtlinien 584
Version der Richtlinie 584
JSON-Richtliniendokument 584
Weitere Informationen 586
AmazonGrafanaCloudWatchAccess 586
Diese Richtlinie wird verwendet 587
Einzelheiten zu den Richtlinien 587
Version der Richtlinie 587
JSON-Richtliniendokument 587
Weitere Informationen 588
AmazonGrafanaRedshiftAccess 589
Diese Richtlinie wird verwendet 589
Einzelheiten zu den Richtlinien 589
Version der Richtlinie 589
JSON-Richtliniendokument 589
Weitere Informationen 591
AmazonGrafanaServiceLinkedRolePolicy 591
Diese Richtlinie wird verwendet 591
Einzelheiten der Richtlinie 591
Version der Richtlinie 591
JSON-Richtliniendokument 592
Weitere Informationen 593
AmazonGuardDutyFullAccess 593
Diese Richtlinie wird verwendet 593
Einzelheiten zu den Richtlinien 593
Version der Richtlinie 594
JSON-Richtliniendokument 594
Weitere Informationen 595
AmazonGuardDutyMalwareProtectionServiceRolePolicy 596
Diese Richtlinie wird verwendet 596
Einzelheiten der Richtlinie 596
Version der Richtlinie 596
JSON-Richtliniendokument 597
Weitere Informationen 601

AmazonGuardDutyReadOnlyAccess 601
Diese Richtlinie wird verwendet 601
Einzelheiten zu den Richtlinien 601
Version der Richtlinie 602
JSON-Richtliniendokument 602
Weitere Informationen 602
AmazonGuardDutyServiceRolePolicy 603
Diese Richtlinie wird verwendet 603
Einzelheiten der Richtlinie 603
Version der Richtlinie 603
JSON-Richtliniendokument 604
Weitere Informationen 610
AmazonHealthLakeFullAccess 610
Diese Richtlinie wird verwendet 610
Einzelheiten zu den Richtlinien 610
Version der Richtlinie 610
JSON-Richtliniendokument 610
Weitere Informationen 611
AmazonHealthLakeReadOnlyAccess 611
Diese Richtlinie wird verwendet 612
Einzelheiten zu den Richtlinien 612
Version der Richtlinie 612
JSON-Richtliniendokument 612
Weitere Informationen 613
AmazonHoneycodeFullAccess 613
Diese Richtlinie wird verwendet 613
Einzelheiten zu den Richtlinien 613
Version der Richtlinie 613
JSON-Richtliniendokument 614
Weitere Informationen 614
AmazonHoneycodeReadOnlyAccess 614
Diese Richtlinie wird verwendet 614
Einzelheiten zu den Richtlinien 615
Version der Richtlinie 615
JSON-Richtliniendokument 615
Weitere Informationen 615

AmazonHoneycodeServiceRolePolicy 616
Diese Richtlinie wird verwendet 616
Einzelheiten der Richtlinie 616
Version der Richtlinie 616
JSON-Richtliniendokument 616
Weitere Informationen 617
AmazonHoneycodeTeamAssociationFullAccess 617
Diese Richtlinie wird verwendet 617
Einzelheiten zu den Richtlinien 617
Version der Richtlinie 618
JSON-Richtliniendokument 618
Weitere Informationen 618
AmazonHoneycodeTeamAssociationReadOnlyAccess 618
Diese Richtlinie wird verwendet 619
Einzelheiten zu den Richtlinien 619
Version der Richtlinie 619
JSON-Richtliniendokument 619
Weitere Informationen 620
AmazonHoneycodeWorkbookFullAccess 620
Diese Richtlinie wird verwendet 620
Einzelheiten zu den Richtlinien 620
Version der Richtlinie 620
JSON-Richtliniendokument 621
Weitere Informationen 621
AmazonHoneycodeWorkbookReadOnlyAccess 621
Diese Richtlinie wird verwendet 622
Einzelheiten zu den Richtlinien 622
Version der Richtlinie 622
JSON-Richtliniendokument 622
Weitere Informationen 623
AmazonInspector2AgentlessServiceRolePolicy 623
Diese Richtlinie wird verwendet 623
Einzelheiten der Richtlinie 623
Version der Richtlinie 623
JSON-Richtliniendokument 624
Weitere Informationen 627

AmazonInspector2FullAccess 627
Diese Richtlinie wird verwendet 628
Einzelheiten zu den Richtlinien 628
Version der Richtlinie 628
JSON-Richtliniendokument 628
Weitere Informationen 629
AmazonInspector2ManagedCisPolicy 630
Diese Richtlinie wird verwendet 630
Einzelheiten zu den Richtlinien 630
Version der Richtlinie 630
JSON-Richtliniendokument 630
Weitere Informationen 631
AmazonInspector2ReadOnlyAccess 631
Diese Richtlinie wird verwendet 631
Einzelheiten zu den Richtlinien 631
Version der Richtlinie 631
JSON-Richtliniendokument 632
Weitere Informationen 632
AmazonInspector2ServiceRolePolicy 633
Diese Richtlinie wird verwendet 633
Einzelheiten der Richtlinie 633
Version der Richtlinie 633
JSON-Richtliniendokument 633
Weitere Informationen 640
AmazonInspectorFullAccess 640
Diese Richtlinie wird verwendet 640
Einzelheiten zu den Richtlinien 640
Version der Richtlinie 640
JSON-Richtliniendokument 641
Weitere Informationen 642
AmazonInspectorReadOnlyAccess 642
Diese Richtlinie wird verwendet 642
Einzelheiten zu den Richtlinien 642
Version der Richtlinie 642
JSON-Richtliniendokument 643
Weitere Informationen 643

AmazonInspectorServiceRolePolicy 643
Diese Richtlinie wird verwendet 644
Einzelheiten der Richtlinie 644
Version der Richtlinie 644
JSON-Richtliniendokument 644
Weitere Informationen 645
AmazonKendraFullAccess 646
Diese Richtlinie wird verwendet 646
Einzelheiten zu den Richtlinien 646
Version der Richtlinie 646
JSON-Richtliniendokument 646
Weitere Informationen 648
AmazonKendraReadOnlyAccess 648
Diese Richtlinie wird verwendet 649
Einzelheiten zu den Richtlinien 649
Version der Richtlinie 649
JSON-Richtliniendokument 649
Weitere Informationen 650
AmazonKeyspacesFullAccess 650
Diese Richtlinie wird verwendet 650
Einzelheiten zu den Richtlinien 650
Version der Richtlinie 650
JSON-Richtliniendokument 651
Weitere Informationen 652
AmazonKeyspacesReadOnlyAccess 653
Diese Richtlinie wird verwendet 653
Einzelheiten zu den Richtlinien 653
Version der Richtlinie 653
JSON-Richtliniendokument 653
Weitere Informationen 654
AmazonKeyspacesReadOnlyAccess_v2 654
Diese Richtlinie wird verwendet 654
Einzelheiten zu den Richtlinien 655
Version der Richtlinie 655
JSON-Richtliniendokument 655
Weitere Informationen 656

AmazonKinesisAnalyticsFullAccess 656
Diese Richtlinie wird verwendet 656
Einzelheiten zu den Richtlinien 656
Version der Richtlinie 657
JSON-Richtliniendokument 657
Weitere Informationen 658
AmazonKinesisAnalyticsReadOnly 658
Diese Richtlinie wird verwendet 659
Einzelheiten zu den Richtlinien 659
Version der Richtlinie 659
JSON-Richtliniendokument 659
Weitere Informationen 660
AmazonKinesisFirehoseFullAccess 661
Diese Richtlinie wird verwendet 661
Einzelheiten zu den Richtlinien 661
Version der Richtlinie 661
JSON-Richtliniendokument 661
Weitere Informationen 662
AmazonKinesisFirehoseReadOnlyAccess 662
Diese Richtlinie wird verwendet 662
Einzelheiten zu den Richtlinien 662
Version der Richtlinie 662
JSON-Richtliniendokument 663
Weitere Informationen 663
AmazonKinesisFullAccess 663
Diese Richtlinie wird verwendet 663
Einzelheiten zu den Richtlinien 664
Version der Richtlinie 664
JSON-Richtliniendokument 664
Weitere Informationen 664
AmazonKinesisReadOnlyAccess 665
Diese Richtlinie wird verwendet 665
Einzelheiten zu den Richtlinien 665
Version der Richtlinie 665
JSON-Richtliniendokument 665
Weitere Informationen 666

AmazonKinesisVideoStreamsFullAccess ... 666
Diese Richtlinie wird verwendet ... 666
Einzelheiten zu den Richtlinien ... 666
Version der Richtlinie ... 666
JSON-Richtliniendokument ... 667
Weitere Informationen ... 667
AmazonKinesisVideoStreamsReadOnlyAccess ... 667
Diese Richtlinie wird verwendet ... 667
Einzelheiten zu den Richtlinien ... 668
Version der Richtlinie ... 668
JSON-Richtliniendokument ... 668
Weitere Informationen ... 668
AmazonLaunchWizard_Fullaccess ... 669
Diese Richtlinie wird verwendet ... 669
Einzelheiten zu den Richtlinien ... 669
Version der Richtlinie ... 669
JSON-Richtliniendokument ... 669
Weitere Informationen ... 683
AmazonLaunchWizardFullAccessV2 ... 684
Diese Richtlinie wird verwendet ... 684
Einzelheiten zu den Richtlinien ... 684
Version der Richtlinie ... 684
JSON-Richtliniendokument ... 684
Weitere Informationen ... 701
AmazonLexChannelsAccess ... 701
Diese Richtlinie wird verwendet ... 701
Einzelheiten der Richtlinie ... 701
Version der Richtlinie ... 702
JSON-Richtliniendokument ... 702
Weitere Informationen ... 702
AmazonLexFullAccess ... 702
Diese Richtlinie wird verwendet ... 703
Einzelheiten zu den Richtlinien ... 703
Version der Richtlinie ... 703
JSON-Richtliniendokument ... 703
Weitere Informationen ... 709

AmazonLexReadOnly ... 709
Diese Richtlinie wird verwendet ... 709
Einzelheiten zu den Richtlinien ... 709
Version der Richtlinie ... 709
JSON-Richtliniendokument ... 710
Weitere Informationen ... 711
AmazonLexReplicationPolicy ... 711
Diese Richtlinie wird verwendet ... 712
Einzelheiten der Richtlinie ... 712
Version der Richtlinie ... 712
JSON-Richtliniendokument ... 712
Weitere Informationen ... 714
AmazonLexRunBotsOnly ... 714
Diese Richtlinie wird verwendet ... 715
Einzelheiten zu den Richtlinien ... 715
Version der Richtlinie ... 715
JSON-Richtliniendokument ... 715
Weitere Informationen ... 716
AmazonLexV2BotPolicy ... 716
Diese Richtlinie wird verwendet ... 716
Einzelheiten der Richtlinie ... 716
Version der Richtlinie ... 716
JSON-Richtliniendokument ... 717
Weitere Informationen ... 717
AmazonLookoutEquipmentFullAccess ... 717
Diese Richtlinie wird verwendet ... 717
Einzelheiten zu den Richtlinien ... 718
Version der Richtlinie ... 718
JSON-Richtliniendokument ... 718
Weitere Informationen ... 719
AmazonLookoutEquipmentReadOnlyAccess ... 719
Diese Richtlinie wird verwendet ... 720
Einzelheiten zu den Richtlinien ... 720
Version der Richtlinie ... 720
JSON-Richtliniendokument ... 720
Weitere Informationen ... 721

AmazonLookoutMetricsFullAccess 721
Diese Richtlinie wird verwendet 721
Einzelheiten zu den Richtlinien 721
Version der Richtlinie 721
JSON-Richtliniendokument 722
Weitere Informationen 722
AmazonLookoutMetricsReadOnlyAccess 722
Diese Richtlinie wird verwendet 723
Einzelheiten zu den Richtlinien 723
Version der Richtlinie 723
JSON-Richtliniendokument 723
Weitere Informationen 724
AmazonLookoutVisionConsoleFullAccess 724
Diese Richtlinie wird verwendet 724
Einzelheiten zu den Richtlinien 724
Version der Richtlinie 725
JSON-Richtliniendokument 725
Weitere Informationen 727
AmazonLookoutVisionConsoleReadOnlyAccess 727
Diese Richtlinie wird verwendet 727
Einzelheiten zu den Richtlinien 727
Version der Richtlinie 728
JSON-Richtliniendokument 728
Weitere Informationen 729
AmazonLookoutVisionFullAccess 729
Diese Richtlinie wird verwendet 730
Einzelheiten zu den Richtlinien 730
Version der Richtlinie 730
JSON-Richtliniendokument 730
Weitere Informationen 731
AmazonLookoutVisionReadOnlyAccess 731
Diese Richtlinie wird verwendet 731
Einzelheiten zu den Richtlinien 731
Version der Richtlinie 731
JSON-Richtliniendokument 732
Weitere Informationen 732

AmazonMachineLearningBatchPredictionsAccess 732
Diese Richtlinie wird verwendet 733
Einzelheiten zu den Richtlinien 733
Version der Richtlinie 733
JSON-Richtliniendokument 733
Weitere Informationen 734
AmazonMachineLearningCreateOnlyAccess 734
Diese Richtlinie wird verwendet 734
Einzelheiten zu den Richtlinien 734
Version der Richtlinie 734
JSON-Richtliniendokument 735
Weitere Informationen 735
AmazonMachineLearningFullAccess 735
Diese Richtlinie wird verwendet 735
Einzelheiten zu den Richtlinien 736
Version der Richtlinie 736
JSON-Richtliniendokument 736
Weitere Informationen 736
AmazonMachineLearningManageRealTimeEndpointOnlyAccess 737
Diese Richtlinie wird verwendet 737
Einzelheiten zu den Richtlinien 737
Version der Richtlinie 737
JSON-Richtliniendokument 737
Weitere Informationen 738
AmazonMachineLearningReadOnlyAccess 738
Diese Richtlinie wird verwendet 738
Einzelheiten zu den Richtlinien 738
Version der Richtlinie 738
JSON-Richtliniendokument 739
Weitere Informationen 739
AmazonMachineLearningRealTimePredictionOnlyAccess 739
Diese Richtlinie wird verwendet 740
Einzelheiten zu den Richtlinien 740
Version der Richtlinie 740
JSON-Richtliniendokument 740
Weitere Informationen 741

AmazonMachineLearningRoleforRedshiftDataSourceV3 741
Diese Richtlinie wird verwendet 741
Einzelheiten zu den Richtlinien 741
Version der Richtlinie 741
JSON-Richtliniendokument 742
Weitere Informationen 742
AmazonMacieFullAccess 743
Diese Richtlinie wird verwendet 743
Einzelheiten zu den Richtlinien 743
Version der Richtlinie 743
JSON-Richtliniendokument 743
Weitere Informationen 744
AmazonMacieHandshakeRole 744
Diese Richtlinie wird verwendet 744
Einzelheiten zu den Richtlinien 745
Version der Richtlinie 745
JSON-Richtliniendokument 745
Weitere Informationen 745
AmazonMacieReadOnlyAccess 746
Diese Richtlinie wird verwendet 746
Einzelheiten zu den Richtlinien 746
Version der Richtlinie 746
JSON-Richtliniendokument 746
Weitere Informationen 747
AmazonMacieServiceRole 747
Diese Richtlinie wird verwendet 747
Einzelheiten zu den Richtlinien 747
Version der Richtlinie 748
JSON-Richtliniendokument 748
Weitere Informationen 748
AmazonMacieServiceRolePolicy 748
Diese Richtlinie wird verwendet 749
Einzelheiten der Richtlinie 749
Version der Richtlinie 749
JSON-Richtliniendokument 749
Weitere Informationen 750

AmazonManagedBlockchainConsoleFullAccess 751
Diese Richtlinie wird verwendet 751
Einzelheiten zu den Richtlinien 751
Version der Richtlinie 751
JSON-Richtliniendokument 751
Weitere Informationen 752
AmazonManagedBlockchainFullAccess 752
Diese Richtlinie wird verwendet 752
Einzelheiten zu den Richtlinien 752
Version der Richtlinie 753
JSON-Richtliniendokument 753
Weitere Informationen 753
AmazonManagedBlockchainReadOnlyAccess 754
Diese Richtlinie wird verwendet 754
Einzelheiten zu den Richtlinien 754
Version der Richtlinie 754
JSON-Richtliniendokument 754
Weitere Informationen 755
AmazonManagedBlockchainServiceRolePolicy 755
Diese Richtlinie wird verwendet 755
Einzelheiten der Richtlinie 755
Version der Richtlinie 755
JSON-Richtliniendokument 756
Weitere Informationen 756
AmazonMCSFullAccess 756
Diese Richtlinie wird verwendet 757
Einzelheiten zu den Richtlinien 757
Version der Richtlinie 757
JSON-Richtliniendokument 757
Weitere Informationen 758
AmazonMCSReadOnlyAccess 759
Diese Richtlinie wird verwendet 759
Einzelheiten zu den Richtlinien 759
Version der Richtlinie 759
JSON-Richtliniendokument 759
Weitere Informationen 760

AmazonMechanicalTurkFullAccess 760
Diese Richtlinie wird verwendet 760
Einzelheiten zu den Richtlinien 760
Version der Richtlinie 761
JSON-Richtliniendokument 761
Weitere Informationen 761
AmazonMechanicalTurkReadOnly 761
Diese Richtlinie wird verwendet 762
Einzelheiten zu den Richtlinien 762
Version der Richtlinie 762
JSON-Richtliniendokument 762
Weitere Informationen 763
AmazonMemoryDBFullAccess 763
Diese Richtlinie wird verwendet 763
Einzelheiten zu den Richtlinien 763
Version der Richtlinie 763
JSON-Richtliniendokument 764
Weitere Informationen 764
AmazonMemoryDBReadOnlyAccess 764
Diese Richtlinie wird verwendet 765
Einzelheiten zu den Richtlinien 765
Version der Richtlinie 765
JSON-Richtliniendokument 765
Weitere Informationen 766
AmazonMobileAnalyticsFinancialReportAccess 766
Diese Richtlinie wird verwendet 766
Einzelheiten zu den Richtlinien 766
Version der Richtlinie 766
JSON-Richtliniendokument 767
Weitere Informationen 767
AmazonMobileAnalyticsFullAccess 767
Diese Richtlinie wird verwendet 767
Einzelheiten zu den Richtlinien 767
Version der Richtlinie 768
JSON-Richtliniendokument 768
Weitere Informationen 768

AmazonMobileAnalyticsNon-financialReportAccess 768
Diese Richtlinie wird verwendet 769
Einzelheiten zu den Richtlinien 769
Version der Richtlinie 769
JSON-Richtliniendokument 769
Weitere Informationen 770
AmazonMobileAnalyticsWriteOnlyAccess 770
Diese Richtlinie wird verwendet 770
Einzelheiten zu den Richtlinien 770
Version der Richtlinie 770
JSON-Richtliniendokument 771
Weitere Informationen 771
AmazonMonitronFullAccess 771
Diese Richtlinie wird verwendet 771
Einzelheiten zu den Richtlinien 771
Version der Richtlinie 772
JSON-Richtliniendokument 772
Weitere Informationen 774
AmazonMQApiFullAccess 774
Diese Richtlinie wird verwendet 774
Einzelheiten zu den Richtlinien 774
Version der Richtlinie 774
JSON-Richtliniendokument 775
Weitere Informationen 776
AmazonMQApiReadOnlyAccess 776
Diese Richtlinie wird verwendet 776
Einzelheiten zu den Richtlinien 776
Version der Richtlinie 776
JSON-Richtliniendokument 777
Weitere Informationen 777
AmazonMQFullAccess 777
Diese Richtlinie wird verwendet 777
Einzelheiten zu den Richtlinien 778
Version der Richtlinie 778
JSON-Richtliniendokument 778
Weitere Informationen 779

AmazonMQReadOnlyAccess 779
Diese Richtlinie wird verwendet 780
Einzelheiten zu den Richtlinien 780
Version der Richtlinie 780
JSON-Richtliniendokument 780
Weitere Informationen 781
AmazonMQServiceRolePolicy 781
Diese Richtlinie wird verwendet 781
Einzelheiten der Richtlinie 781
Version der Richtlinie 781
JSON-Richtliniendokument 782
Weitere Informationen 783
AmazonMSKConnectReadOnlyAccess 784
Diese Richtlinie wird verwendet 784
Einzelheiten zu den Richtlinien 784
Version der Richtlinie 784
JSON-Richtliniendokument 784
Weitere Informationen 785
AmazonMSKFullAccess 786
Diese Richtlinie wird verwendet 786
Einzelheiten zu den Richtlinien 786
Version der Richtlinie 786
JSON-Richtliniendokument 786
Weitere Informationen 789
AmazonMSKReadOnlyAccess 789
Diese Richtlinie wird verwendet 789
Einzelheiten zu den Richtlinien 790
Version der Richtlinie 790
JSON-Richtliniendokument 790
Weitere Informationen 791
AmazonMWAAServiceRolePolicy 791
Diese Richtlinie wird verwendet 791
Einzelheiten der Richtlinie 791
Version der Richtlinie 791
JSON-Richtliniendokument 792
Weitere Informationen 794

AmazonNimbleStudio-LaunchProfileWorker 794
Diese Richtlinie wird verwendet 794
Einzelheiten zu den Richtlinien 794
Version der Richtlinie 794
JSON-Richtliniendokument 795
Weitere Informationen 795
AmazonNimbleStudio-StudioAdmin 796
Diese Richtlinie wird verwendet 796
Einzelheiten zu den Richtlinien 796
Version der Richtlinie 796
JSON-Richtliniendokument 796
Weitere Informationen 798
AmazonNimbleStudio-StudioUser 798
Diese Richtlinie wird verwendet 799
Einzelheiten zu den Richtlinien 799
Version der Richtlinie 799
JSON-Richtliniendokument 799
Weitere Informationen 801
AmazonOmicsFullAccess 801
Diese Richtlinie wird verwendet 802
Einzelheiten zu den Richtlinien 802
Version der Richtlinie 802
JSON-Richtliniendokument 802
Weitere Informationen 803
AmazonOmicsReadOnlyAccess 803
Diese Richtlinie wird verwendet 803
Einzelheiten zu den Richtlinien 804
Version der Richtlinie 804
JSON-Richtliniendokument 804
Weitere Informationen 804
AmazonOneEnterpriseFullAccess 805
Diese Richtlinie wird verwendet 805
Einzelheiten zu den Richtlinien 805
Version der Richtlinie 805
JSON-Richtliniendokument 805
Weitere Informationen 806

AmazonOneEnterpriseInstallerAccess 806
Diese Richtlinie wird verwendet 806
Einzelheiten zu den Richtlinien 806
Version der Richtlinie 807
JSON-Richtliniendokument 807
Weitere Informationen 807
AmazonOneEnterpriseReadOnlyAccess 808
Diese Richtlinie wird verwendet 808
Einzelheiten zu den Richtlinien 808
Version der Richtlinie 808
JSON-Richtliniendokument 808
Weitere Informationen 809
AmazonOpenSearchDashboardsServiceRolePolicy 809
Diese Richtlinie wird verwendet 809
Einzelheiten der Richtlinie 809
Version der Richtlinie 810
JSON-Richtliniendokument 810
Weitere Informationen 810
AmazonOpenSearchDirectQueryGlueCreateAccess 810
Diese Richtlinie wird verwendet 811
Einzelheiten zu den Richtlinien 811
Version der Richtlinie 811
JSON-Richtliniendokument 811
Weitere Informationen 812
AmazonOpenSearchIngestionFullAccess 812
Diese Richtlinie wird verwendet 812
Einzelheiten zu den Richtlinien 812
Version der Richtlinie 812
JSON-Richtliniendokument 813
Weitere Informationen 813
AmazonOpenSearchIngestionReadOnlyAccess 814
Diese Richtlinie wird verwendet 814
Einzelheiten zu den Richtlinien 814
Version der Richtlinie 814
JSON-Richtliniendokument 814
Weitere Informationen 815

AmazonOpenSearchIngestionServiceRolePolicy 815
Diese Richtlinie wird verwendet 815
Einzelheiten der Richtlinie 815
Version der Richtlinie 816
JSON-Richtliniendokument 816
Weitere Informationen 818
AmazonOpenSearchServerlessServiceRolePolicy 818
Diese Richtlinie wird verwendet 818
Einzelheiten der Richtlinie 818
Version der Richtlinie 818
JSON-Richtliniendokument 819
Weitere Informationen 819
AmazonOpenSearchServiceCognitoAccess 819
Diese Richtlinie wird verwendet 819
Einzelheiten zu den Richtlinien 820
Version der Richtlinie 820
JSON-Richtliniendokument 820
Weitere Informationen 821
AmazonOpenSearchServiceFullAccess 821
Diese Richtlinie wird verwendet 821
Einzelheiten zu den Richtlinien 822
Version der Richtlinie 822
JSON-Richtliniendokument 822
Weitere Informationen 822
AmazonOpenSearchServiceReadOnlyAccess 823
Diese Richtlinie wird verwendet 823
Einzelheiten zu den Richtlinien 823
Version der Richtlinie 823
JSON-Richtliniendokument 823
Weitere Informationen 824
AmazonOpenSearchServiceRolePolicy 824
Diese Richtlinie wird verwendet 824
Einzelheiten der Richtlinie 824
Version der Richtlinie 824
JSON-Richtliniendokument 825
Weitere Informationen 829

AmazonPersonalizeFullAccess 829
Diese Richtlinie wird verwendet 830
Einzelheiten zu den Richtlinien 830
Version der Richtlinie 830
JSON-Richtliniendokument 830
Weitere Informationen 831
AmazonPollyFullAccess 831
Diese Richtlinie wird verwendet 832
Einzelheiten zu den Richtlinien 832
Version der Richtlinie 832
JSON-Richtliniendokument 832
Weitere Informationen 833
AmazonPollyReadOnlyAccess 833
Diese Richtlinie wird verwendet 833
Einzelheiten zu den Richtlinien 833
Version der Richtlinie 833
JSON-Richtliniendokument 834
Weitere Informationen 834
AmazonPrometheusConsoleFullAccess 834
Diese Richtlinie wird verwendet 835
Einzelheiten zu den Richtlinien 835
Version der Richtlinie 835
JSON-Richtliniendokument 835
Weitere Informationen 836
AmazonPrometheusFullAccess 836
Diese Richtlinie wird verwendet 837
Einzelheiten zu den Richtlinien 837
Version der Richtlinie 837
JSON-Richtliniendokument 837
Weitere Informationen 838
AmazonPrometheusQueryAccess 838
Diese Richtlinie wird verwendet 839
Einzelheiten zu den Richtlinien 839
Version der Richtlinie 839
JSON-Richtliniendokument 839
Weitere Informationen 840

AmazonPrometheusRemoteWriteAccess 840
Diese Richtlinie wird verwendet 840
Einzelheiten zu den Richtlinien 840
Version der Richtlinie 840
JSON-Richtliniendokument 841
Weitere Informationen 841
AmazonPrometheusScraperServiceRolePolicy 841
Diese Richtlinie wird verwendet 841
Einzelheiten der Richtlinie 841
Version der Richtlinie 842
JSON-Richtliniendokument 842
Weitere Informationen 844
AmazonQFullAccess 844
Diese Richtlinie wird verwendet 845
Einzelheiten zu den Richtlinien 845
Version der Richtlinie 845
JSON-Richtliniendokument 845
Weitere Informationen 846
AmazonQLDBConsoleFullAccess 846
Diese Richtlinie wird verwendet 846
Einzelheiten zu den Richtlinien 846
Version der Richtlinie 846
JSON-Richtliniendokument 847
Weitere Informationen 848
AmazonQLDBFullAccess 849
Diese Richtlinie wird verwendet 849
Einzelheiten zu den Richtlinien 849
Version der Richtlinie 849
JSON-Richtliniendokument 849
Weitere Informationen 851
AmazonQLDBReadOnly 851
Diese Richtlinie wird verwendet 851
Einzelheiten zu den Richtlinien 851
Version der Richtlinie 851
JSON-Richtliniendokument 852
Weitere Informationen 852

AmazonRDSBetaServiceRolePolicy 852
Diese Richtlinie wird verwendet 853
Einzelheiten der Richtlinie 853
Version der Richtlinie 853
JSON-Richtliniendokument 853
Weitere Informationen 856
AmazonRDSCustomInstanceProfileRolePolicy 856
Diese Richtlinie wird verwendet 857
Einzelheiten zu den Richtlinien 857
Version der Richtlinie 857
JSON-Richtliniendokument 857
Weitere Informationen 864
AmazonRDSCustomPreviewServiceRolePolicy 865
Diese Richtlinie wird verwendet 865
Einzelheiten der Richtlinie 865
Version der Richtlinie 865
JSON-Richtliniendokument 865
Weitere Informationen 881
AmazonRDSCustomServiceRolePolicy 881
Diese Richtlinie wird verwendet 881
Einzelheiten der Richtlinie 881
Version der Richtlinie 882
JSON-Richtliniendokument 882
Weitere Informationen 899
AmazonRDSDataFullAccess 899
Diese Richtlinie wird verwendet 899
Einzelheiten zu den Richtlinien 900
Version der Richtlinie 900
JSON-Richtliniendokument 900
Weitere Informationen 901
AmazonRDSDirectoryServiceAccess 901
Diese Richtlinie wird verwendet 902
Einzelheiten zu den Richtlinien 902
Version der Richtlinie 902
JSON-Richtliniendokument 902
Weitere Informationen 903

AmazonRDSEnhancedMonitoringRole ... 903
Diese Richtlinie wird verwendet ... 903
Einzelheiten zu den Richtlinien ... 903
Version der Richtlinie ... 903
JSON-Richtliniendokument ... 904
Weitere Informationen ... 904
AmazonRDSFullAccess ... 905
Diese Richtlinie wird verwendet ... 905
Einzelheiten zu den Richtlinien ... 905
Version der Richtlinie ... 905
JSON-Richtliniendokument ... 905
Weitere Informationen ... 907
AmazonRDSPerformanceInsightsFullAccess ... 908
Diese Richtlinie wird verwendet ... 908
Einzelheiten zu den Richtlinien ... 908
Version der Richtlinie ... 908
JSON-Richtliniendokument ... 908
Weitere Informationen ... 910
AmazonRDSPerformanceInsightsReadOnly ... 910
Diese Richtlinie wird verwendet ... 910
Einzelheiten zu den Richtlinien ... 910
Version der Richtlinie ... 910
JSON-Richtliniendokument ... 911
Weitere Informationen ... 912
AmazonRDSPreviewServiceRolePolicy ... 913
Diese Richtlinie wird verwendet ... 913
Einzelheiten der Richtlinie ... 913
Version der Richtlinie ... 913
JSON-Richtliniendokument ... 913
Weitere Informationen ... 916
AmazonRDSReadOnlyAccess ... 917
Diese Richtlinie wird verwendet ... 917
Einzelheiten zu den Richtlinien ... 917
Version der Richtlinie ... 917
JSON-Richtliniendokument ... 917
Weitere Informationen ... 919

AmazonRDSServiceRolePolicy 919
Diese Richtlinie wird verwendet 919
Einzelheiten der Richtlinie 919
Version der Richtlinie 919
JSON-Richtliniendokument 920
Weitere Informationen 924
AmazonRedshiftAllCommandsFullAccess 924
Diese Richtlinie wird verwendet 924
Einzelheiten zu den Richtlinien 924
Version der Richtlinie 924
JSON-Richtliniendokument 925
Weitere Informationen 930
AmazonRedshiftDataFullAccess 930
Diese Richtlinie wird verwendet 930
Einzelheiten zu den Richtlinien 930
Version der Richtlinie 931
JSON-Richtliniendokument 931
Weitere Informationen 933
AmazonRedshiftFullAccess 933
Diese Richtlinie wird verwendet 933
Einzelheiten zu den Richtlinien 933
Version der Richtlinie 933
JSON-Richtliniendokument 934
Weitere Informationen 936
AmazonRedshiftQueryEditor 936
Diese Richtlinie wird verwendet 936
Einzelheiten zu den Richtlinien 936
Version der Richtlinie 936
JSON-Richtliniendokument 937
Weitere Informationen 938
AmazonRedshiftQueryEditorV2FullAccess 939
Diese Richtlinie wird verwendet 939
Einzelheiten zu den Richtlinien 939
Version der Richtlinie 939
JSON-Richtliniendokument 940
Weitere Informationen 941

AmazonRedshiftQueryEditorV2NoSharing 941
Diese Richtlinie wird verwendet 941
Einzelheiten zu den Richtlinien 942
Version der Richtlinie 942
JSON-Richtliniendokument 942
Weitere Informationen 946
AmazonRedshiftQueryEditorV2ReadSharing 946
Diese Richtlinie wird verwendet 946
Einzelheiten zu den Richtlinien 946
Version der Richtlinie 946
JSON-Richtliniendokument 947
Weitere Informationen 952
AmazonRedshiftQueryEditorV2ReadWriteSharing 952
Diese Richtlinie wird verwendet 952
Einzelheiten zu den Richtlinien 952
Version der Richtlinie 952
JSON-Richtliniendokument 953
Weitere Informationen 958
AmazonRedshiftReadOnlyAccess 958
Diese Richtlinie wird verwendet 958
Einzelheiten zu den Richtlinien 958
Version der Richtlinie 958
JSON-Richtliniendokument 959
Weitere Informationen 959
AmazonRedshiftServiceLinkedRolePolicy 960
Diese Richtlinie wird verwendet 960
Einzelheiten der Richtlinie 960
Version der Richtlinie 960
JSON-Richtliniendokument 960
Weitere Informationen 966
AmazonRekognitionCustomLabelsFullAccess 966
Diese Richtlinie wird verwendet 966
Einzelheiten zu den Richtlinien 966
Version der Richtlinie 966
JSON-Richtliniendokument 967
Weitere Informationen 968

AmazonRekognitionFullAccess 968
Diese Richtlinie wird verwendet 968
Einzelheiten zu den Richtlinien 968
Version der Richtlinie 968
JSON-Richtliniendokument 969
Weitere Informationen 969
AmazonRekognitionReadOnlyAccess 969
Diese Richtlinie wird verwendet 969
Einzelheiten zu den Richtlinien 970
Version der Richtlinie 970
JSON-Richtliniendokument 970
Weitere Informationen 971
AmazonRekognitionServiceRole 971
Diese Richtlinie wird verwendet 972
Einzelheiten zu den Richtlinien 972
Version der Richtlinie 972
JSON-Richtliniendokument 972
Weitere Informationen 973
AmazonRoute53AutoNamingFullAccess 973
Diese Richtlinie wird verwendet 973
Einzelheiten zu den Richtlinien 973
Version der Richtlinie 974
JSON-Richtliniendokument 974
Weitere Informationen 974
AmazonRoute53AutoNamingReadOnlyAccess 975
Diese Richtlinie wird verwendet 975
Einzelheiten zu den Richtlinien 975
Version der Richtlinie 975
JSON-Richtliniendokument 975
Weitere Informationen 976
AmazonRoute53AutoNamingRegistrantAccess 976
Diese Richtlinie wird verwendet 976
Einzelheiten zu den Richtlinien 976
Version der Richtlinie 977
JSON-Richtliniendokument 977
Weitere Informationen 977

AmazonRoute53DomainsFullAccess 978
Diese Richtlinie wird verwendet 978
Einzelheiten zu den Richtlinien 978
Version der Richtlinie 978
JSON-Richtliniendokument 978
Weitere Informationen 979
AmazonRoute53DomainsReadOnlyAccess 979
Diese Richtlinie wird verwendet 979
Einzelheiten zu den Richtlinien 979
Version der Richtlinie 980
JSON-Richtliniendokument 980
Weitere Informationen 980
AmazonRoute53FullAccess 980
Diese Richtlinie wird verwendet 981
Einzelheiten zu den Richtlinien 981
Version der Richtlinie 981
JSON-Richtliniendokument 981
Weitere Informationen 982
AmazonRoute53ProfilesFullAccess 982
Diese Richtlinie wird verwendet 982
Einzelheiten zu den Richtlinien 982
Version der Richtlinie 983
JSON-Richtliniendokument 983
Weitere Informationen 984
AmazonRoute53ProfilesReadOnlyAccess 984
Diese Richtlinie wird verwendet 984
Einzelheiten zu den Richtlinien 984
Version der Richtlinie 985
JSON-Richtliniendokument 985
Weitere Informationen 985
AmazonRoute53ReadOnlyAccess 986
Diese Richtlinie wird verwendet 986
Einzelheiten zu den Richtlinien 986
Version der Richtlinie 986
JSON-Richtliniendokument 986
Weitere Informationen 987

AmazonRoute53RecoveryClusterFullAccess 987
Diese Richtlinie wird verwendet 987
Einzelheiten zu den Richtlinien 987
Version der Richtlinie 988
JSON-Richtliniendokument 988
Weitere Informationen 988
AmazonRoute53RecoveryClusterReadOnlyAccess 988
Diese Richtlinie wird verwendet 989
Einzelheiten zu den Richtlinien 989
Version der Richtlinie 989
JSON-Richtliniendokument 989
Weitere Informationen 990
AmazonRoute53RecoveryControlConfigFullAccess 990
Diese Richtlinie wird verwendet 990
Einzelheiten zu den Richtlinien 990
Version der Richtlinie 990
JSON-Richtliniendokument 991
Weitere Informationen 991
AmazonRoute53RecoveryControlConfigReadOnlyAccess 991
Diese Richtlinie wird verwendet 991
Einzelheiten zu den Richtlinien 991
Version der Richtlinie 992
JSON-Richtliniendokument 992
Weitere Informationen 993
AmazonRoute53RecoveryReadinessFullAccess 993
Diese Richtlinie wird verwendet 993
Einzelheiten zu den Richtlinien 993
Version der Richtlinie 993
JSON-Richtliniendokument 994
Weitere Informationen 994
AmazonRoute53RecoveryReadinessReadOnlyAccess 994
Diese Richtlinie wird verwendet 994
Einzelheiten zu den Richtlinien 994
Version der Richtlinie 995
JSON-Richtliniendokument 995
Weitere Informationen 996

AmazonRoute53ResolverFullAccess 996
Diese Richtlinie wird verwendet 996
Einzelheiten zu den Richtlinien 996
Version der Richtlinie 996
JSON-Richtliniendokument 997
Weitere Informationen 997
AmazonRoute53ResolverReadOnlyAccess 998
Diese Richtlinie wird verwendet 998
Einzelheiten zu den Richtlinien 998
Version der Richtlinie 998
JSON-Richtliniendokument 998
Weitere Informationen 999
AmazonS3FullAccess 999
Diese Richtlinie wird verwendet 999
Einzelheiten zu den Richtlinien 999
Version der Richtlinie 1000
JSON-Richtliniendokument 1000
Weitere Informationen 1000
AmazonS3ObjectLambdaExecutionRolePolicy 1000
Diese Richtlinie wird verwendet 1001
Einzelheiten zu den Richtlinien 1001
Version der Richtlinie 1001
JSON-Richtliniendokument 1001
Weitere Informationen 1002
AmazonS3OutpostsFullAccess 1002
Diese Richtlinie wird verwendet 1002
Einzelheiten zu den Richtlinien 1002
Version der Richtlinie 1002
JSON-Richtliniendokument 1003
Weitere Informationen 1004
AmazonS3OutpostsReadOnlyAccess 1004
Diese Richtlinie wird verwendet 1004
Einzelheiten zu den Richtlinien 1004
Version der Richtlinie 1004
JSON-Richtliniendokument 1005
Weitere Informationen 1006

AmazonS3ReadOnlyAccess 1006
Diese Richtlinie wird verwendet 1006
Einzelheiten zu den Richtlinien 1006
Version der Richtlinie 1006
JSON-Richtliniendokument 1007
Weitere Informationen 1007
AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 1007
Diese Richtlinie wird verwendet 1008
Einzelheiten zu den Richtlinien 1008
Version der Richtlinie 1008
JSON-Richtliniendokument 1008
Weitere Informationen 1018
AmazonSageMakerCanvasAIServicesAccess 1018
Diese Richtlinie wird verwendet 1019
Einzelheiten zu den Richtlinien 1019
Version der Richtlinie 1019
JSON-Richtliniendokument 1019
Weitere Informationen 1022
AmazonSageMakerCanvasBedrockAccess 1022
Diese Richtlinie wird verwendet 1023
Einzelheiten zu den Richtlinien 1023
Version der Richtlinie 1023
JSON-Richtliniendokument 1023
Weitere Informationen 1024
AmazonSageMakerCanvasDataPrepFullAccess 1024
Diese Richtlinie wird verwendet 1024
Einzelheiten zu den Richtlinien 1024
Version der Richtlinie 1025
JSON-Richtliniendokument 1025
Weitere Informationen 1032
AmazonSageMakerCanvasDirectDeployAccess 1032
Diese Richtlinie wird verwendet 1032
Einzelheiten zu den Richtlinien 1032
Version der Richtlinie 1033
JSON-Richtliniendokument 1033
Weitere Informationen 1034

AmazonSageMakerCanvasForecastAccess 1034
Diese Richtlinie wird verwendet 1034
Einzelheiten zu den Richtlinien 1034
Version der Richtlinie 1034
JSON-Richtliniendokument 1035
Weitere Informationen 1035
AmazonSageMakerCanvasFullAccess 1036
Diese Richtlinie wird verwendet 1036
Einzelheiten zu den Richtlinien 1036
Version der Richtlinie 1036
JSON-Richtliniendokument 1036
Weitere Informationen 1044
AmazonSageMakerClusterInstanceRolePolicy 1044
Diese Richtlinie wird verwendet 1045
Einzelheiten zu den Richtlinien 1045
Version der Richtlinie 1045
JSON-Richtliniendokument 1045
Weitere Informationen 1047
AmazonSageMakerCoreServiceRolePolicy 1047
Diese Richtlinie wird verwendet 1047
Einzelheiten der Richtlinie 1047
Version der Richtlinie 1048
JSON-Richtliniendokument 1048
Weitere Informationen 1049
AmazonSageMakerEdgeDeviceFleetPolicy 1049
Diese Richtlinie wird verwendet 1049
Einzelheiten zu den Richtlinien 1049
Version der Richtlinie 1050
JSON-Richtliniendokument 1050
Weitere Informationen 1052
AmazonSageMakerFeatureStoreAccess 1052
Diese Richtlinie wird verwendet 1052
Einzelheiten zu den Richtlinien 1052
Version der Richtlinie 1052
JSON-Richtliniendokument 1053
Weitere Informationen 1054

AmazonSageMakerFullAccess 1054
Diese Richtlinie wird verwendet 1054
Einzelheiten zu den Richtlinien 1054
Version der Richtlinie 1054
JSON-Richtliniendokument 1055
Weitere Informationen 1071
AmazonSageMakerGeospatialExecutionRole 1071
Diese Richtlinie wird verwendet 1071
Einzelheiten zu den Richtlinien 1071
Version der Richtlinie 1071
JSON-Richtliniendokument 1072
Weitere Informationen 1072
AmazonSageMakerGeospatialFullAccess 1073
Diese Richtlinie wird verwendet 1073
Einzelheiten zu den Richtlinien 1073
Version der Richtlinie 1073
JSON-Richtliniendokument 1073
Weitere Informationen 1074
AmazonSageMakerGroundTruthExecution 1074
Diese Richtlinie wird verwendet 1074
Einzelheiten zu den Richtlinien 1074
Version der Richtlinie 1075
JSON-Richtliniendokument 1075
Weitere Informationen 1078
AmazonSageMakerMechanicalTurkAccess 1079
Diese Richtlinie wird verwendet 1079
Einzelheiten zu den Richtlinien 1079
Version der Richtlinie 1079
JSON-Richtliniendokument 1079
Weitere Informationen 1080
AmazonSageMakerModelGovernanceUseAccess 1080
Diese Richtlinie wird verwendet 1080
Einzelheiten zu den Richtlinien 1080
Version der Richtlinie 1080
JSON-Richtliniendokument 1081
Weitere Informationen 1083

AmazonSageMakerModelRegistryFullAccess 1083
Diese Richtlinie wird verwendet 1083
Einzelheiten zu den Richtlinien 1083
Version der Richtlinie 1083
JSON-Richtliniendokument 1084
Weitere Informationen 1087
AmazonSageMakerNotebooksServiceRolePolicy 1087
Diese Richtlinie wird verwendet 1088
Einzelheiten der Richtlinie 1088
Version der Richtlinie 1088
JSON-Richtliniendokument 1088
Weitere Informationen 1092
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 1092
Diese Richtlinie wird verwendet 1093
Einzelheiten zu den Richtlinien 1093
Version der Richtlinie 1093
JSON-Richtliniendokument 1093
Weitere Informationen 1094
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 1094
Diese Richtlinie wird verwendet 1095
Einzelheiten zu den Richtlinien 1095
Version der Richtlinie 1095
JSON-Richtliniendokument 1095
Weitere Informationen 1099
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1099
Diese Richtlinie wird verwendet 1099
Einzelheiten zu den Richtlinien 1099
Version der Richtlinie 1099
JSON-Richtliniendokument 1100
Weitere Informationen 1100
AmazonSageMakerPipelinesIntegrations 1100
Diese Richtlinie wird verwendet 1101
Einzelheiten zu den Richtlinien 1101
Version der Richtlinie 1101
JSON-Richtliniendokument 1101
Weitere Informationen 1103

AmazonSageMakerReadOnly 1103
Diese Richtlinie wird verwendet 1103
Einzelheiten zu den Richtlinien 1103
Version der Richtlinie 1104
JSON-Richtliniendokument 1104
Weitere Informationen 1105
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1105
Diese Richtlinie wird verwendet 1106
Einzelheiten zu den Richtlinien 1106
Version der Richtlinie 1106
JSON-Richtliniendokument 1106
Weitere Informationen 1107
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1107
Diese Richtlinie wird verwendet 1107
Einzelheiten zu den Richtlinien 1108
Version der Richtlinie 1108
JSON-Richtliniendokument 1108
Weitere Informationen 1115
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1115
Diese Richtlinie wird verwendet 1115
Einzelheiten zu den Richtlinien 1115
Version der Richtlinie 1116
JSON-Richtliniendokument 1116
Weitere Informationen 1126
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1126
Diese Richtlinie wird verwendet 1126
Einzelheiten zu den Richtlinien 1127
Version der Richtlinie 1127
JSON-Richtliniendokument 1127
Weitere Informationen 1130
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1130
Diese Richtlinie wird verwendet 1130
Einzelheiten zu den Richtlinien 1130
Version der Richtlinie 1131
JSON-Richtliniendokument 1131
Weitere Informationen 1131

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1131
Diese Richtlinie wird verwendet 1132
Einzelheiten zu den Richtlinien 1132
Version der Richtlinie 1132
JSON-Richtliniendokument 1132
Weitere Informationen 1133
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1133
Diese Richtlinie wird verwendet 1133
Einzelheiten zu den Richtlinien 1133
Version der Richtlinie 1133
JSON-Richtliniendokument 1134
Weitere Informationen 1136
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1136
Diese Richtlinie wird verwendet 1136
Einzelheiten zu den Richtlinien 1136
Version der Richtlinie 1137
JSON-Richtliniendokument 1137
Weitere Informationen 1147
AmazonSecurityLakeAdministrator 1147
Diese Richtlinie wird verwendet 1147
Einzelheiten zu den Richtlinien 1147
Version der Richtlinie 1148
JSON-Richtliniendokument 1148
Weitere Informationen 1159
AmazonSecurityLakeMetastoreManager 1159
Diese Richtlinie wird verwendet 1159
Einzelheiten zu den Richtlinien 1159
Version der Richtlinie 1160
JSON-Richtliniendokument 1160
Weitere Informationen 1162
AmazonSecurityLakePermissionsBoundary 1162
Diese Richtlinie wird verwendet 1163
Einzelheiten zu den Richtlinien 1163
Version der Richtlinie 1163
JSON-Richtliniendokument 1163
Weitere Informationen 1166

AmazonSESFullAccess 1166
Diese Richtlinie wird verwendet 1167
Einzelheiten zu den Richtlinien 1167
Version der Richtlinie 1167
JSON-Richtliniendokument 1167
Weitere Informationen 1168
AmazonSESReadOnlyAccess 1168
Diese Richtlinie wird verwendet 1168
Einzelheiten zu den Richtlinien 1168
Version der Richtlinie 1168
JSON-Richtliniendokument 1169
Weitere Informationen 1169
AmazonSESServiceRolePolicy 1169
Diese Richtlinie wird verwendet 1169
Einzelheiten der Richtlinie 1170
Version der Richtlinie 1170
JSON-Richtliniendokument 1170
Weitere Informationen 1171
AmazonSNSFullAccess 1171
Diese Richtlinie wird verwendet 1171
Einzelheiten zu den Richtlinien 1171
Version der Richtlinie 1171
JSON-Richtliniendokument 1171
Weitere Informationen 1172
AmazonSNSReadOnlyAccess 1172
Diese Richtlinie wird verwendet 1172
Einzelheiten zu den Richtlinien 1172
Version der Richtlinie 1173
JSON-Richtliniendokument 1173
Weitere Informationen 1173
AmazonSNSRole 1173
Diese Richtlinie wird verwendet 1174
Einzelheiten zu den Richtlinien 1174
Version der Richtlinie 1174
JSON-Richtliniendokument 1174
Weitere Informationen 1175

AmazonSQSFullAccess 1175
Diese Richtlinie wird verwendet 1175
Einzelheiten zu den Richtlinien 1175
Version der Richtlinie 1175
JSON-Richtliniendokument 1176
Weitere Informationen 1176
AmazonSQSReadOnlyAccess 1176
Diese Richtlinie wird verwendet 1176
Einzelheiten zu den Richtlinien 1176
Version der Richtlinie 1177
JSON-Richtliniendokument 1177
Weitere Informationen 1177
AmazonSSMAutomationApproverAccess 1178
Diese Richtlinie wird verwendet 1178
Einzelheiten zu den Richtlinien 1178
Version der Richtlinie 1178
JSON-Richtliniendokument 1178
Weitere Informationen 1179
AmazonSSMAutomationRole 1179
Diese Richtlinie wird verwendet 1179
Einzelheiten zu den Richtlinien 1179
Version der Richtlinie 1180
JSON-Richtliniendokument 1180
Weitere Informationen 1181
AmazonSSMDirectoryServiceAccess 1181
Diese Richtlinie wird verwendet 1182
Einzelheiten zu den Richtlinien 1182
Version der Richtlinie 1182
JSON-Richtliniendokument 1182
Weitere Informationen 1183
AmazonSSMFullAccess 1183
Diese Richtlinie wird verwendet 1183
Einzelheiten zu den Richtlinien 1183
Version der Richtlinie 1183
JSON-Richtliniendokument 1184
Weitere Informationen 1185

AmazonSSMMaintenanceWindowRole 1185
Diese Richtlinie wird verwendet 1185
Einzelheiten zu den Richtlinien 1185
Version der Richtlinie 1185
JSON-Richtliniendokument 1186
Weitere Informationen 1187
AmazonSSMManagedEC2InstanceDefaultPolicy 1187
Diese Richtlinie wird verwendet 1188
Einzelheiten zu den Richtlinien 1188
Version der Richtlinie 1188
JSON-Richtliniendokument 1188
Weitere Informationen 1189
AmazonSSMManagedInstanceCore 1190
Diese Richtlinie wird verwendet 1190
Einzelheiten zu den Richtlinien 1190
Version der Richtlinie 1190
JSON-Richtliniendokument 1190
Weitere Informationen 1191
AmazonSSMPatchAssociation 1192
Diese Richtlinie wird verwendet 1192
Einzelheiten zu den Richtlinien 1192
Version der Richtlinie 1192
JSON-Richtliniendokument 1192
Weitere Informationen 1193
AmazonSSMReadOnlyAccess 1193
Diese Richtlinie wird verwendet 1193
Einzelheiten zu den Richtlinien 1194
Version der Richtlinie 1194
JSON-Richtliniendokument 1194
Weitere Informationen 1194
AmazonSSMServiceRolePolicy 1195
Diese Richtlinie wird verwendet 1195
Einzelheiten der Richtlinie 1195
Version der Richtlinie 1195
JSON-Richtliniendokument 1195
Weitere Informationen 1200

AmazonSumerianFullAccess 1201
Diese Richtlinie wird verwendet 1201
Einzelheiten zu den Richtlinien 1201
Version der Richtlinie 1201
JSON-Richtliniendokument 1201
Weitere Informationen 1202
AmazonTextractFullAccess 1202
Diese Richtlinie wird verwendet 1202
Einzelheiten zu den Richtlinien 1202
Version der Richtlinie 1202
JSON-Richtliniendokument 1203
Weitere Informationen 1203
AmazonTextractServiceRole 1203
Diese Richtlinie wird verwendet 1203
Einzelheiten zu den Richtlinien 1204
Version der Richtlinie 1204
JSON-Richtliniendokument 1204
Weitere Informationen 1204
AmazonTimestreamConsoleFullAccess 1205
Diese Richtlinie wird verwendet 1205
Einzelheiten zu den Richtlinien 1205
Version der Richtlinie 1205
JSON-Richtliniendokument 1205
Weitere Informationen 1207
AmazonTimestreamFullAccess 1207
Diese Richtlinie wird verwendet 1208
Einzelheiten zu den Richtlinien 1208
Version der Richtlinie 1208
JSON-Richtliniendokument 1208
Weitere Informationen 1209
AmazonTimestreamInfluxDBFullAccess 1210
Diese Richtlinie wird verwendet 1210
Einzelheiten zu den Richtlinien 1210
Version der Richtlinie 1210
JSON-Richtliniendokument 1210
Weitere Informationen 1212

AmazonTimestreamInfluxDBServiceRolePolicy 1212
Diese Richtlinie wird verwendet 1213
Einzelheiten der Richtlinie 1213
Version der Richtlinie 1213
JSON-Richtliniendokument 1213
Weitere Informationen 1216
AmazonTimestreamReadOnlyAccess 1216
Diese Richtlinie wird verwendet 1216
Einzelheiten zu den Richtlinien 1216
Version der Richtlinie 1216
JSON-Richtliniendokument 1217
Weitere Informationen 1217
AmazonTranscribeFullAccess 1218
Diese Richtlinie wird verwendet 1218
Einzelheiten zu den Richtlinien 1218
Version der Richtlinie 1218
JSON-Richtliniendokument 1218
Weitere Informationen 1219
AmazonTranscribeReadOnlyAccess 1219
Diese Richtlinie wird verwendet 1219
Einzelheiten zu den Richtlinien 1219
Version der Richtlinie 1220
JSON-Richtliniendokument 1220
Weitere Informationen 1220
AmazonVPCCrossAccountNetworkInterfaceOperations 1220
Diese Richtlinie wird verwendet 1221
Einzelheiten zu den Richtlinien 1221
Version der Richtlinie 1221
JSON-Richtliniendokument 1221
Weitere Informationen 1223
AmazonVPCFullAccess 1223
Diese Richtlinie wird verwendet 1223
Einzelheiten zu den Richtlinien 1223
Version der Richtlinie 1223
JSON-Richtliniendokument 1224
Weitere Informationen 1227

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1228
Diese Richtlinie wird verwendet 1228
Einzelheiten zu den Richtlinien 1228
Version der Richtlinie 1228
JSON-Richtliniendokument 1228
Weitere Informationen 1232
AmazonVPCReachabilityAnalyzerFullAccessPolicy 1232
Diese Richtlinie wird verwendet 1232
Einzelheiten zu den Richtlinien 1232
Version der Richtlinie 1232
JSON-Richtliniendokument 1233
Weitere Informationen 1236
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1236
Diese Richtlinie wird verwendet 1236
Einzelheiten zu den Richtlinien 1236
Version der Richtlinie 1237
JSON-Richtliniendokument 1237
Weitere Informationen 1237
AmazonVPCReadOnlyAccess 1237
Diese Richtlinie wird verwendet 1238
Einzelheiten zu den Richtlinien 1238
Version der Richtlinie 1238
JSON-Richtliniendokument 1238
Weitere Informationen 1239
AmazonWorkDocsFullAccess 1240
Diese Richtlinie wird verwendet 1240
Einzelheiten zu den Richtlinien 1240
Version der Richtlinie 1240
JSON-Richtliniendokument 1240
Weitere Informationen 1241
AmazonWorkDocsReadOnlyAccess 1241
Diese Richtlinie wird verwendet 1241
Einzelheiten zu den Richtlinien 1241
Version der Richtlinie 1242
JSON-Richtliniendokument 1242
Weitere Informationen 1242

AmazonWorkMailEventsServiceRolePolicy 1242
Diese Richtlinie wird verwendet 1243
Einzelheiten der Richtlinie 1243
Version der Richtlinie 1243
JSON-Richtliniendokument 1243
Weitere Informationen 1244
AmazonWorkMailFullAccess 1244
Diese Richtlinie wird verwendet 1244
Einzelheiten zu den Richtlinien 1244
Version der Richtlinie 1244
JSON-Richtliniendokument 1245
Weitere Informationen 1247
AmazonWorkMailMessageFlowFullAccess 1247
Diese Richtlinie wird verwendet 1247
Einzelheiten zu den Richtlinien 1247
Version der Richtlinie 1247
JSON-Richtliniendokument 1248
Weitere Informationen 1248
AmazonWorkMailMessageFlowReadOnlyAccess 1248
Diese Richtlinie wird verwendet 1248
Einzelheiten zu den Richtlinien 1248
Version der Richtlinie 1249
JSON-Richtliniendokument 1249
Weitere Informationen 1249
AmazonWorkMailReadOnlyAccess 1249
Diese Richtlinie wird verwendet 1250
Einzelheiten zu den Richtlinien 1250
Version der Richtlinie 1250
JSON-Richtliniendokument 1250
Weitere Informationen 1251
AmazonWorkSpacesAdmin 1251
Diese Richtlinie wird verwendet 1251
Einzelheiten zu den Richtlinien 1251
Version der Richtlinie 1251
JSON-Richtliniendokument 1252
Weitere Informationen 1253

AmazonWorkSpacesApplicationManagerAdminAccess 1253
Diese Richtlinie wird verwendet 1253
Einzelheiten zu den Richtlinien 1253
Version der Richtlinie 1253
JSON-Richtliniendokument 1254
Weitere Informationen 1254
AmazonWorkspacesPCAAccess 1254
Diese Richtlinie wird verwendet 1254
Einzelheiten zu den Richtlinien 1254
Version der Richtlinie 1255
JSON-Richtliniendokument 1255
Weitere Informationen 1255
AmazonWorkSpacesSelfServiceAccess 1256
Diese Richtlinie wird verwendet 1256
Einzelheiten zu den Richtlinien 1256
Version der Richtlinie 1256
JSON-Richtliniendokument 1256
Weitere Informationen 1257
AmazonWorkSpacesServiceAccess 1257
Diese Richtlinie wird verwendet 1257
Einzelheiten zu den Richtlinien 1257
Version der Richtlinie 1258
JSON-Richtliniendokument 1258
Weitere Informationen 1258
AmazonWorkSpacesWebReadOnly 1258
Diese Richtlinie wird verwendet 1259
Einzelheiten zu den Richtlinien 1259
Version der Richtlinie 1259
JSON-Richtliniendokument 1259
Weitere Informationen 1260
AmazonWorkSpacesWebServiceRolePolicy 1260
Diese Richtlinie wird verwendet 1261
Einzelheiten der Richtlinie 1261
Version der Richtlinie 1261
JSON-Richtliniendokument 1261
Weitere Informationen 1263

AmazonZocaloFullAccess 1264
Diese Richtlinie wird verwendet 1264
Einzelheiten zu den Richtlinien 1264
Version der Richtlinie 1264
JSON-Richtliniendokument 1264
Weitere Informationen 1265
AmazonZocaloReadOnlyAccess 1265
Diese Richtlinie wird verwendet 1265
Einzelheiten zu den Richtlinien 1266
Version der Richtlinie 1266
JSON-Richtliniendokument 1266
Weitere Informationen 1266
AmplifyBackendDeployFullAccess 1267
Diese Richtlinie wird verwendet 1267
Einzelheiten zu den Richtlinien 1267
Version der Richtlinie 1267
JSON-Richtliniendokument 1267
Weitere Informationen 1271
APIGatewayServiceRolePolicy 1272
Diese Richtlinie wird verwendet 1272
Einzelheiten der Richtlinie 1272
Version der Richtlinie 1272
JSON-Richtliniendokument 1272
Weitere Informationen 1275
AppIntegrationsServiceLinkedRolePolicy 1275
Diese Richtlinie wird verwendet 1275
Einzelheiten der Richtlinie 1275
Version der Richtlinie 1275
JSON-Richtliniendokument 1276
Weitere Informationen 1277
ApplicationAutoScalingForAmazonAppStreamAccess 1277
Diese Richtlinie wird verwendet 1277
Einzelheiten zu den Richtlinien 1278
Version der Richtlinie 1278
JSON-Richtliniendokument 1278
Weitere Informationen 1279

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1279
Diese Richtlinie wird verwendet 1279
Einzelheiten der Richtlinie 1279
Version der Richtlinie 1279
JSON-Richtliniendokument 1280
Weitere Informationen 1282
AppRunnerNetworkingServiceRolePolicy 1282
Diese Richtlinie wird verwendet 1282
Einzelheiten der Richtlinie 1282
Version der Richtlinie 1282
JSON-Richtliniendokument 1283
Weitere Informationen 1284
AppRunnerServiceRolePolicy 1284
Diese Richtlinie wird verwendet 1284
Einzelheiten der Richtlinie 1284
Version der Richtlinie 1285
JSON-Richtliniendokument 1285
Weitere Informationen 1286
AutoScalingConsoleFullAccess 1286
Diese Richtlinie wird verwendet 1286
Einzelheiten zu den Richtlinien 1286
Version der Richtlinie 1286
JSON-Richtliniendokument 1287
Weitere Informationen 1288
AutoScalingConsoleReadOnlyAccess 1289
Diese Richtlinie wird verwendet 1289
Einzelheiten zu den Richtlinien 1289
Version der Richtlinie 1289
JSON-Richtliniendokument 1289
Weitere Informationen 1290
AutoScalingFullAccess 1291
Diese Richtlinie wird verwendet 1291
Einzelheiten zu den Richtlinien 1291
Version der Richtlinie 1291
JSON-Richtliniendokument 1291
Weitere Informationen 1293

AutoScalingNotificationAccessRole 1293
Diese Richtlinie wird verwendet 1293
Einzelheiten zu den Richtlinien 1293
Version der Richtlinie 1293
JSON-Richtliniendokument 1294
Weitere Informationen 1294
AutoScalingReadOnlyAccess 1294
Diese Richtlinie wird verwendet 1294
Einzelheiten zu den Richtlinien 1294
Version der Richtlinie 1295
JSON-Richtliniendokument 1295
Weitere Informationen 1295
AutoScalingServiceRolePolicy 1296
Diese Richtlinie wird verwendet 1296
Einzelheiten der Richtlinie 1296
Version der Richtlinie 1296
JSON-Richtliniendokument 1296
Weitere Informationen 1299
AWS_ConfigRole 1299
Diese Richtlinie wird verwendet 1299
Einzelheiten zu den Richtlinien 1300
Version der Richtlinie 1300
JSON-Richtliniendokument 1300
Weitere Informationen 1331
AWSAccountActivityAccess 1331
Diese Richtlinie wird verwendet 1331
Einzelheiten zu den Richtlinien 1331
Version der Richtlinie 1331
JSON-Richtliniendokument 1332
Weitere Informationen 1332
AWSAccountManagementFullAccess 1333
Diese Richtlinie wird verwendet 1333
Einzelheiten zu den Richtlinien 1333
Version der Richtlinie 1333
JSON-Richtliniendokument 1333
Weitere Informationen 1334

AWSAccountManagementReadOnlyAccess 1334
Diese Richtlinie wird verwendet 1334
Einzelheiten zu den Richtlinien 1334
Version der Richtlinie 1334
JSON-Richtliniendokument 1335
Weitere Informationen 1335
AWSAccountUsageReportAccess 1335
Diese Richtlinie wird verwendet 1335
Einzelheiten zu den Richtlinien 1335
Version der Richtlinie 1336
JSON-Richtliniendokument 1336
Weitere Informationen 1336
AWSAgentlessDiscoveryService 1337
Diese Richtlinie wird verwendet 1337
Einzelheiten zu den Richtlinien 1337
Version der Richtlinie 1337
JSON-Richtliniendokument 1337
Weitere Informationen 1339
AWSAppFabricFullAccess 1339
Diese Richtlinie wird verwendet 1340
Einzelheiten zu den Richtlinien 1340
Version der Richtlinie 1340
JSON-Richtliniendokument 1340
Weitere Informationen 1341
AWSAppFabricReadOnlyAccess 1342
Diese Richtlinie wird verwendet 1342
Einzelheiten zu den Richtlinien 1342
Version der Richtlinie 1342
JSON-Richtliniendokument 1342
Weitere Informationen 1343
AWSAppFabricServiceRolePolicy 1343
Diese Richtlinie wird verwendet 1343
Einzelheiten der Richtlinie 1343
Version der Richtlinie 1344
JSON-Richtliniendokument 1344
Weitere Informationen 1345

AWSApplicationAutoscalingAppStreamFleetPolicy 1345
Diese Richtlinie wird verwendet 1345
Einzelheiten der Richtlinie 1345
Version der Richtlinie 1346
JSON-Richtliniendokument 1346
Weitere Informationen 1346
AWSApplicationAutoscalingCassandraTablePolicy 1347
Diese Richtlinie wird verwendet 1347
Einzelheiten der Richtlinie 1347
Version der Richtlinie 1347
JSON-Richtliniendokument 1347
Weitere Informationen 1348
AWSApplicationAutoscalingComprehendEndpointPolicy 1348
Diese Richtlinie wird verwendet 1348
Einzelheiten der Richtlinie 1348
Version der Richtlinie 1349
JSON-Richtliniendokument 1349
Weitere Informationen 1349
AWSApplicationAutoScalingCustomResourcePolicy 1350
Diese Richtlinie wird verwendet 1350
Einzelheiten der Richtlinie 1350
Version der Richtlinie 1350
JSON-Richtliniendokument 1350
Weitere Informationen 1351
AWSApplicationAutoscalingDynamoDBTablePolicy 1351
Diese Richtlinie wird verwendet 1351
Einzelheiten der Richtlinie 1351
Version der Richtlinie 1352
JSON-Richtliniendokument 1352
Weitere Informationen 1352
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1353
Diese Richtlinie wird verwendet 1353
Einzelheiten der Richtlinie 1353
Version der Richtlinie 1353
JSON-Richtliniendokument 1353
Weitere Informationen 1354

AWSApplicationAutoscalingECSServicePolicy 1354
Diese Richtlinie wird verwendet 1354
Einzelheiten der Richtlinie 1354
Version der Richtlinie 1355
JSON-Richtliniendokument 1355
Weitere Informationen 1355
AWSApplicationAutoscalingElastiCacheRGPolicy 1355
Diese Richtlinie wird verwendet 1356
Einzelheiten der Richtlinie 1356
Version der Richtlinie 1356
JSON-Richtliniendokument 1356
Weitere Informationen 1357
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1357
Diese Richtlinie wird verwendet 1357
Einzelheiten der Richtlinie 1357
Version der Richtlinie 1358
JSON-Richtliniendokument 1358
Weitere Informationen 1358
AWSApplicationAutoscalingKafkaClusterPolicy 1359
Diese Richtlinie wird verwendet 1359
Einzelheiten der Richtlinie 1359
Version der Richtlinie 1359
JSON-Richtliniendokument 1359
Weitere Informationen 1360
AWSApplicationAutoscalingLambdaConcurrencyPolicy 1360
Diese Richtlinie wird verwendet 1360
Einzelheiten der Richtlinie 1360
Version der Richtlinie 1361
JSON-Richtliniendokument 1361
Weitere Informationen 1361
AWSApplicationAutoscalingNeptuneClusterPolicy 1362
Diese Richtlinie wird verwendet 1362
Einzelheiten der Richtlinie 1362
Version der Richtlinie 1362
JSON-Richtliniendokument 1362
Weitere Informationen 1364

AWSApplicationAutoscalingRDSClusterPolicy 1364
Diese Richtlinie wird verwendet 1364
Einzelheiten der Richtlinie 1364
Version der Richtlinie 1365
JSON-Richtliniendokument 1365
Weitere Informationen 1366
AWSApplicationAutoscalingSageMakerEndpointPolicy 1366
Diese Richtlinie wird verwendet 1366
Einzelheiten der Richtlinie 1366
Version der Richtlinie 1366
JSON-Richtliniendokument 1367
Weitere Informationen 1367
AWSApplicationDiscoveryAgentAccess 1368
Diese Richtlinie wird verwendet 1368
Einzelheiten zu den Richtlinien 1368
Version der Richtlinie 1368
JSON-Richtliniendokument 1368
Weitere Informationen 1369
AWSApplicationDiscoveryAgentlessCollectorAccess 1369
Diese Richtlinie wird verwendet 1369
Einzelheiten zu den Richtlinien 1369
Version der Richtlinie 1370
JSON-Richtliniendokument 1370
Weitere Informationen 1371
AWSApplicationDiscoveryServiceFullAccess 1371
Diese Richtlinie wird verwendet 1371
Einzelheiten zu den Richtlinien 1371
Version der Richtlinie 1372
JSON-Richtliniendokument 1372
Weitere Informationen 1373
AWSApplicationMigrationAgentInstallationPolicy 1373
Diese Richtlinie wird verwendet 1374
Einzelheiten zu den Richtlinien 1374
Version der Richtlinie 1374
JSON-Richtliniendokument 1374
Weitere Informationen 1375

AWSApplicationMigrationAgentPolicy 1375
Diese Richtlinie wird verwendet 1376
Einzelheiten zu den Richtlinien 1376
Version der Richtlinie 1376
JSON-Richtliniendokument 1376
Weitere Informationen 1377
AWSApplicationMigrationAgentPolicy_v2 1377
Diese Richtlinie wird verwendet 1378
Einzelheiten zu den Richtlinien 1378
Version der Richtlinie 1378
JSON-Richtliniendokument 1378
Weitere Informationen 1379
AWSApplicationMigrationConversionServerPolicy 1379
Diese Richtlinie wird verwendet 1379
Einzelheiten zu den Richtlinien 1379
Version der Richtlinie 1380
JSON-Richtliniendokument 1380
Weitere Informationen 1380
AWSApplicationMigrationEC2Access 1381
Diese Richtlinie wird verwendet 1381
Einzelheiten zu den Richtlinien 1381
Version der Richtlinie 1381
JSON-Richtliniendokument 1381
Weitere Informationen 1389
AWSApplicationMigrationFullAccess 1389
Diese Richtlinie wird verwendet 1389
Einzelheiten zu den Richtlinien 1390
Version der Richtlinie 1390
JSON-Richtliniendokument 1390
Weitere Informationen 1396
AWSApplicationMigrationMGHAccess 1396
Diese Richtlinie wird verwendet 1396
Einzelheiten zu den Richtlinien 1397
Version der Richtlinie 1397
JSON-Richtliniendokument 1397
Weitere Informationen 1398

AWSApplicationMigrationReadOnlyAccess 1398
Diese Richtlinie wird verwendet 1398
Einzelheiten zu den Richtlinien 1398
Version der Richtlinie 1398
JSON-Richtliniendokument 1399
Weitere Informationen 1400
AWSApplicationMigrationReplicationServerPolicy 1400
Diese Richtlinie wird verwendet 1400
Einzelheiten zu den Richtlinien 1400
Version der Richtlinie 1401
JSON-Richtliniendokument 1401
Weitere Informationen 1402
AWSApplicationMigrationServiceEc2InstancePolicy 1403
Diese Richtlinie wird verwendet 1403
Einzelheiten zu den Richtlinien 1403
Version der Richtlinie 1403
JSON-Richtliniendokument 1404
Weitere Informationen 1405
AWSApplicationMigrationServiceRolePolicy 1405
Diese Richtlinie wird verwendet 1405
Einzelheiten der Richtlinie 1405
Version der Richtlinie 1405
JSON-Richtliniendokument 1406
Weitere Informationen 1413
AWSApplicationMigrationSSMAccess 1413
Diese Richtlinie wird verwendet 1413
Einzelheiten zu den Richtlinien 1413
Version der Richtlinie 1413
JSON-Richtliniendokument 1414
Weitere Informationen 1415
AWSApplicationMigrationVCenterClientPolicy 1416
Diese Richtlinie wird verwendet 1416
Einzelheiten zu den Richtlinien 1416
Version der Richtlinie 1416
JSON-Richtliniendokument 1416
Weitere Informationen 1417

AWSAppMeshEnvoyAccess 1417
Diese Richtlinie wird verwendet 1418
Einzelheiten zu den Richtlinien 1418
Version der Richtlinie 1418
JSON-Richtliniendokument 1418
Weitere Informationen 1418
AWSAppMeshFullAccess 1419
Diese Richtlinie wird verwendet 1419
Einzelheiten zu den Richtlinien 1419
Version der Richtlinie 1419
JSON-Richtliniendokument 1419
Weitere Informationen 1421
AWSAppMeshPreviewEnvoyAccess 1421
Diese Richtlinie wird verwendet 1421
Einzelheiten zu den Richtlinien 1421
Version der Richtlinie 1422
JSON-Richtliniendokument 1422
Weitere Informationen 1422
AWSAppMeshPreviewServiceRolePolicy 1422
Diese Richtlinie wird verwendet 1423
Einzelheiten der Richtlinie 1423
Version der Richtlinie 1423
JSON-Richtliniendokument 1423
Weitere Informationen 1424
AWSAppMeshReadOnly 1424
Diese Richtlinie wird verwendet 1424
Einzelheiten zu den Richtlinien 1424
Version der Richtlinie 1424
JSON-Richtliniendokument 1425
Weitere Informationen 1426
AWSAppMeshServiceRolePolicy 1426
Diese Richtlinie wird verwendet 1426
Einzelheiten der Richtlinie 1426
Version der Richtlinie 1426
JSON-Richtliniendokument 1427
Weitere Informationen 1427

AWSAppRunnerFullAccess 1427
Diese Richtlinie wird verwendet 1428
Einzelheiten zu den Richtlinien 1428
Version der Richtlinie 1428
JSON-Richtliniendokument 1428
Weitere Informationen 1429
AWSAppRunnerReadOnlyAccess 1429
Diese Richtlinie wird verwendet 1429
Einzelheiten zu den Richtlinien 1430
Version der Richtlinie 1430
JSON-Richtliniendokument 1430
Weitere Informationen 1430
AWSAppRunnerServicePolicyForECRAccess 1431
Diese Richtlinie wird verwendet 1431
Einzelheiten zu den Richtlinien 1431
Version der Richtlinie 1431
JSON-Richtliniendokument 1431
Weitere Informationen 1432
AWSAppSyncAdministrator 1432
Diese Richtlinie wird verwendet 1432
Einzelheiten zu den Richtlinien 1432
Version der Richtlinie 1433
JSON-Richtliniendokument 1433
Weitere Informationen 1434
AWSAppSyncInvokeFullAccess 1434
Diese Richtlinie wird verwendet 1434
Einzelheiten zu den Richtlinien 1435
Version der Richtlinie 1435
JSON-Richtliniendokument 1435
Weitere Informationen 1435
AWSAppSyncPushToCloudWatchLogs 1436
Diese Richtlinie wird verwendet 1436
Einzelheiten zu den Richtlinien 1436
Version der Richtlinie 1436
JSON-Richtliniendokument 1436
Weitere Informationen 1437

AWSAppSyncSchemaAuthor 1437
Diese Richtlinie wird verwendet 1437
Einzelheiten zu den Richtlinien 1437
Version der Richtlinie 1438
JSON-Richtliniendokument 1438
Weitere Informationen 1439
AWSAppSyncServiceRolePolicy 1439
Diese Richtlinie wird verwendet 1439
Einzelheiten der Richtlinie 1439
Version der Richtlinie 1440
JSON-Richtliniendokument 1440
Weitere Informationen 1440
AWSArtifactAccountSync 1440
Diese Richtlinie wird verwendet 1441
Einzelheiten zu den Richtlinien 1441
Version der Richtlinie 1441
JSON-Richtliniendokument 1441
Weitere Informationen 1442
AWSArtifactReportsReadOnlyAccess 1442
Diese Richtlinie wird verwendet 1442
Einzelheiten zu den Richtlinien 1442
Version der Richtlinie 1442
JSON-Richtliniendokument 1443
Weitere Informationen 1443
AWSArtifactServiceRolePolicy 1443
Diese Richtlinie wird verwendet 1444
Einzelheiten der Richtlinie 1444
Version der Richtlinie 1444
JSON-Richtliniendokument 1444
Weitere Informationen 1445
AWSAuditManagerAdministratorAccess 1445
Diese Richtlinie wird verwendet 1445
Einzelheiten zu den Richtlinien 1445
Version der Richtlinie 1445
JSON-Richtliniendokument 1446
Weitere Informationen 1450

AWSAuditManagerServiceRolePolicy 1450
Diese Richtlinie wird verwendet 1450
Einzelheiten der Richtlinie 1450
Version der Richtlinie 1450
JSON-Richtliniendokument 1451
Weitere Informationen 1457
AWSAutoScalingPlansEC2AutoScalingPolicy 1458
Diese Richtlinie wird verwendet 1458
Einzelheiten der Richtlinie 1458
Version der Richtlinie 1458
JSON-Richtliniendokument 1458
Weitere Informationen 1459
AWSBackupAuditAccess 1459
Diese Richtlinie wird verwendet 1459
Einzelheiten zu den Richtlinien 1459
Version der Richtlinie 1460
JSON-Richtliniendokument 1460
Weitere Informationen 1461
AWSBackupDataTransferAccess 1461
Diese Richtlinie wird verwendet 1462
Einzelheiten zu den Richtlinien 1462
Version der Richtlinie 1462
JSON-Richtliniendokument 1462
Weitere Informationen 1463
AWSBackupFullAccess 1463
Diese Richtlinie wird verwendet 1463
Einzelheiten zu den Richtlinien 1463
Version der Richtlinie 1463
JSON-Richtliniendokument 1464
Weitere Informationen 1473
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 1474
Diese Richtlinie wird verwendet 1474
Einzelheiten zu den Richtlinien 1474
Version der Richtlinie 1474
JSON-Richtliniendokument 1474
Weitere Informationen 1475

AWSBackupOperatorAccess 1475
Diese Richtlinie wird verwendet 1475
Einzelheiten zu den Richtlinien 1476
Version der Richtlinie 1476
JSON-Richtliniendokument 1476
Weitere Informationen 1483
AWSBackupOrganizationAdminAccess 1483
Diese Richtlinie wird verwendet 1483
Einzelheiten zu den Richtlinien 1483
Version der Richtlinie 1483
JSON-Richtliniendokument 1484
Weitere Informationen 1486
AWSBackupRestoreAccessForSAPHANA 1486
Diese Richtlinie wird verwendet 1486
Einzelheiten zu den Richtlinien 1486
Version der Richtlinie 1486
JSON-Richtliniendokument 1487
Weitere Informationen 1487
AWSBackupServiceLinkedRolePolicyForBackup 1488
Diese Richtlinie wird verwendet 1488
Einzelheiten der Richtlinie 1488
Version der Richtlinie 1488
JSON-Richtliniendokument 1488
Weitere Informationen 1496
AWSBackupServiceLinkedRolePolicyForBackupTest 1497
Diese Richtlinie wird verwendet 1497
Einzelheiten der Richtlinie 1497
Version der Richtlinie 1497
JSON-Richtliniendokument 1497
Weitere Informationen 1498
AWSBackupServiceRolePolicyForBackup 1498
Diese Richtlinie wird verwendet 1498
Einzelheiten zu den Richtlinien 1498
Version der Richtlinie 1499
JSON-Richtliniendokument 1499
Weitere Informationen 1510

AWSBackupServiceRolePolicyForRestores 1510
Diese Richtlinie wird verwendet 1510
Einzelheiten zu den Richtlinien 1510
Version der Richtlinie 1511
JSON-Richtliniendokument 1511
Weitere Informationen 1521
AWSBackupServiceRolePolicyForS3Backup 1521
Diese Richtlinie wird verwendet 1521
Einzelheiten zu den Richtlinien 1521
Version der Richtlinie 1521
JSON-Richtliniendokument 1522
Weitere Informationen 1524
AWSBackupServiceRolePolicyForS3Restore 1524
Diese Richtlinie wird verwendet 1524
Einzelheiten zu den Richtlinien 1525
Version der Richtlinie 1525
JSON-Richtliniendokument 1525
Weitere Informationen 1526
AWSBatchFullAccess 1527
Diese Richtlinie wird verwendet 1527
Einzelheiten zu den Richtlinien 1527
Version der Richtlinie 1527
JSON-Richtliniendokument 1527
Weitere Informationen 1529
AWSBatchServiceEventTargetRole 1529
Diese Richtlinie wird verwendet 1529
Einzelheiten zu den Richtlinien 1529
Version der Richtlinie 1529
JSON-Richtliniendokument 1530
Weitere Informationen 1530
AWSBatchServiceRole 1530
Diese Richtlinie wird verwendet 1530
Einzelheiten zu den Richtlinien 1531
Version der Richtlinie 1531
JSON-Richtliniendokument 1531
Weitere Informationen 1534

AWSBCMDataExportsServiceRolePolicy 1534
Diese Richtlinie wird verwendet 1535
Einzelheiten der Richtlinie 1535
Version der Richtlinie 1535
JSON-Richtliniendokument 1535
Weitere Informationen 1536
AWSBillingConductorFullAccess 1536
Diese Richtlinie wird verwendet 1536
Einzelheiten zu den Richtlinien 1536
Version der Richtlinie 1536
JSON-Richtliniendokument 1537
Weitere Informationen 1537
AWSBillingConductorReadOnlyAccess 1537
Diese Richtlinie wird verwendet 1537
Einzelheiten zu den Richtlinien 1538
Version der Richtlinie 1538
JSON-Richtliniendokument 1538
Weitere Informationen 1538
AWSBillingReadOnlyAccess 1539
Diese Richtlinie wird verwendet 1539
Einzelheiten zu den Richtlinien 1539
Version der Richtlinie 1539
JSON-Richtliniendokument 1539
Weitere Informationen 1541
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 1541
Diese Richtlinie wird verwendet 1541
Einzelheiten zu den Richtlinien 1541
Version der Richtlinie 1542
JSON-Richtliniendokument 1542
Weitere Informationen 1543
AWSBudgetsActionsWithAWSResourceControlAccess 1543
Diese Richtlinie wird verwendet 1543
Einzelheiten zu den Richtlinien 1543
Version der Richtlinie 1544
JSON-Richtliniendokument 1544
Weitere Informationen 1545

AWSBudgetsReadOnlyAccess 1545
Diese Richtlinie wird verwendet 1546
Einzelheiten zu den Richtlinien 1546
Version der Richtlinie 1546
JSON-Richtliniendokument 1546
Weitere Informationen 1547
AWSBugBustFullAccess 1547
Diese Richtlinie wird verwendet 1547
Einzelheiten zu den Richtlinien 1547
Version der Richtlinie 1547
JSON-Richtliniendokument 1548
Weitere Informationen 1549
AWSBugBustPlayerAccess 1549
Diese Richtlinie wird verwendet 1549
Einzelheiten zu den Richtlinien 1549
Version der Richtlinie 1549
JSON-Richtliniendokument 1550
Weitere Informationen 1551
AWSBugBustServiceRolePolicy 1551
Diese Richtlinie wird verwendet 1551
Einzelheiten der Richtlinie 1551
Version der Richtlinie 1551
JSON-Richtliniendokument 1552
Weitere Informationen 1552
AWSCertificateManagerFullAccess 1552
Diese Richtlinie wird verwendet 1552
Einzelheiten zu den Richtlinien 1553
Version der Richtlinie 1553
JSON-Richtliniendokument 1553
Weitere Informationen 1554
AWSCertificateManagerPrivateCAAuditor 1554
Diese Richtlinie wird verwendet 1554
Einzelheiten zu den Richtlinien 1554
Version der Richtlinie 1555
JSON-Richtliniendokument 1555
Weitere Informationen 1555

AWSCertificateManagerPrivateCAFullAccess 1556
Diese Richtlinie wird verwendet 1556
Einzelheiten zu den Richtlinien 1556
Version der Richtlinie 1556
JSON-Richtliniendokument 1556
Weitere Informationen 1557
AWSCertificateManagerPrivateCAPrivilegedUser 1557
Diese Richtlinie wird verwendet 1557
Einzelheiten zu den Richtlinien 1557
Version der Richtlinie 1558
JSON-Richtliniendokument 1558
Weitere Informationen 1559
AWSCertificateManagerPrivateCAReadOnly 1559
Diese Richtlinie wird verwendet 1559
Einzelheiten zu den Richtlinien 1560
Version der Richtlinie 1560
JSON-Richtliniendokument 1560
Weitere Informationen 1561
AWSCertificateManagerPrivateCAUser 1561
Diese Richtlinie wird verwendet 1561
Einzelheiten zu den Richtlinien 1561
Version der Richtlinie 1561
JSON-Richtliniendokument 1562
Weitere Informationen 1563
AWSCertificateManagerReadOnly 1563
Diese Richtlinie wird verwendet 1563
Einzelheiten zu den Richtlinien 1563
Version der Richtlinie 1563
JSON-Richtliniendokument 1564
Weitere Informationen 1564
AWSChatbotServiceLinkedRolePolicy 1564
Diese Richtlinie wird verwendet 1565
Einzelheiten der Richtlinie 1565
Version der Richtlinie 1565
JSON-Richtliniendokument 1565
Weitere Informationen 1566

AWSCleanRoomsFullAccess 1566
Diese Richtlinie wird verwendet 1566
Einzelheiten zu den Richtlinien 1566
Version der Richtlinie 1567
JSON-Richtliniendokument 1567
Weitere Informationen 1571
AWSCleanRoomsFullAccessNoQuerying 1571
Diese Richtlinie wird verwendet 1572
Einzelheiten zu den Richtlinien 1572
Version der Richtlinie 1572
JSON-Richtliniendokument 1572
Weitere Informationen 1577
AWSCleanRoomsMLFullAccess 1577
Diese Richtlinie wird verwendet 1577
Einzelheiten zu den Richtlinien 1577
Version der Richtlinie 1578
JSON-Richtliniendokument 1578
Weitere Informationen 1581
AWSCleanRoomsMLReadOnlyAccess 1582
Diese Richtlinie wird verwendet 1582
Einzelheiten zu den Richtlinien 1582
Version der Richtlinie 1582
JSON-Richtliniendokument 1582
Weitere Informationen 1583
AWSCleanRoomsReadOnlyAccess 1583
Diese Richtlinie wird verwendet 1584
Einzelheiten zu den Richtlinien 1584
Version der Richtlinie 1584
JSON-Richtliniendokument 1584
Weitere Informationen 1585
AWSCloud9Administrator 1586
Diese Richtlinie wird verwendet 1586
Einzelheiten zu den Richtlinien 1586
Version der Richtlinie 1586
JSON-Richtliniendokument 1586
Weitere Informationen 1588

AWSCloud9EnvironmentMember 1588
Diese Richtlinie wird verwendet 1588
Einzelheiten zu den Richtlinien 1588
Version der Richtlinie 1588
JSON-Richtliniendokument 1589
Weitere Informationen 1590
AWSCloud9ServiceRolePolicy 1590
Diese Richtlinie wird verwendet 1590
Einzelheiten der Richtlinie 1591
Version der Richtlinie 1591
JSON-Richtliniendokument 1591
Weitere Informationen 1593
AWSCloud9SSMInstanceProfile 1594
Diese Richtlinie wird verwendet 1594
Einzelheiten zu den Richtlinien 1594
Version der Richtlinie 1594
JSON-Richtliniendokument 1594
Weitere Informationen 1595
AWSCloud9User 1595
Diese Richtlinie wird verwendet 1595
Einzelheiten zu den Richtlinien 1595
Version der Richtlinie 1595
JSON-Richtliniendokument 1596
Weitere Informationen 1598
AWSCloudFormationFullAccess 1598
Diese Richtlinie wird verwendet 1598
Einzelheiten zu den Richtlinien 1598
Version der Richtlinie 1599
JSON-Richtliniendokument 1599
Weitere Informationen 1599
AWSCloudFormationReadOnlyAccess 1600
Diese Richtlinie wird verwendet 1600
Einzelheiten zu den Richtlinien 1600
Version der Richtlinie 1600
JSON-Richtliniendokument 1600
Weitere Informationen 1601

AWSCloudFrontLogger 1601
Diese Richtlinie wird verwendet 1601
Einzelheiten der Richtlinie 1601
Version der Richtlinie 1601
JSON-Richtliniendokument 1602
Weitere Informationen 1602
AWSCloudHSMFullAccess 1602
Diese Richtlinie wird verwendet 1602
Einzelheiten zu den Richtlinien 1603
Version der Richtlinie 1603
JSON-Richtliniendokument 1603
Weitere Informationen 1603
AWSCloudHSMReadOnlyAccess 1604
Diese Richtlinie wird verwendet 1604
Einzelheiten zu den Richtlinien 1604
Version der Richtlinie 1604
JSON-Richtliniendokument 1604
Weitere Informationen 1605
AWSCloudHSMRole 1605
Diese Richtlinie wird verwendet 1605
Einzelheiten zu den Richtlinien 1605
Version der Richtlinie 1605
JSON-Richtliniendokument 1606
Weitere Informationen 1606
AWSCloudMapDiscoverInstanceAccess 1606
Diese Richtlinie wird verwendet 1607
Einzelheiten zu den Richtlinien 1607
Version der Richtlinie 1607
JSON-Richtliniendokument 1607
Weitere Informationen 1608
AWSCloudMapFullAccess 1608
Diese Richtlinie wird verwendet 1608
Einzelheiten zu den Richtlinien 1608
Version der Richtlinie 1608
JSON-Richtliniendokument 1609
Weitere Informationen 1609

AWSCloudMapReadOnlyAccess 1609
Diese Richtlinie wird verwendet 1610
Einzelheiten zu den Richtlinien 1610
Version der Richtlinie 1610
JSON-Richtliniendokument 1610
Weitere Informationen 1611
AWSCloudMapRegisterInstanceAccess 1611
Diese Richtlinie wird verwendet 1611
Einzelheiten zu den Richtlinien 1611
Version der Richtlinie 1611
JSON-Richtliniendokument 1612
Weitere Informationen 1612
AWSCloudShellFullAccess 1613
Diese Richtlinie wird verwendet 1613
Einzelheiten zu den Richtlinien 1613
Version der Richtlinie 1613
JSON-Richtliniendokument 1613
Weitere Informationen 1614
AWSCloudTrail_FullAccess 1614
Diese Richtlinie wird verwendet 1614
Einzelheiten zu den Richtlinien 1614
Version der Richtlinie 1614
JSON-Richtliniendokument 1615
Weitere Informationen 1617
AWSCloudTrail_ReadOnlyAccess 1617
Diese Richtlinie wird verwendet 1618
Einzelheiten zu den Richtlinien 1618
Version der Richtlinie 1618
JSON-Richtliniendokument 1618
Weitere Informationen 1619
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 1619
Diese Richtlinie wird verwendet 1619
Einzelheiten der Richtlinie 1619
Version der Richtlinie 1619
JSON-Richtliniendokument 1620
Weitere Informationen 1620

AWSCodeArtifactAdminAccess 1620
Diese Richtlinie wird verwendet 1620
Einzelheiten zu den Richtlinien 1620
Version der Richtlinie 1621
JSON-Richtliniendokument 1621
Weitere Informationen 1622
AWSCodeArtifactReadOnlyAccess 1622
Diese Richtlinie wird verwendet 1622
Einzelheiten zu den Richtlinien 1622
Version der Richtlinie 1622
JSON-Richtliniendokument 1623
Weitere Informationen 1623
AWSCodeBuildAdminAccess 1624
Diese Richtlinie wird verwendet 1624
Einzelheiten zu den Richtlinien 1624
Version der Richtlinie 1624
JSON-Richtliniendokument 1624
Weitere Informationen 1628
AWSCodeBuildDeveloperAccess 1628
Diese Richtlinie wird verwendet 1628
Einzelheiten zu den Richtlinien 1628
Version der Richtlinie 1628
JSON-Richtliniendokument 1629
Weitere Informationen 1631
AWSCodeBuildReadOnlyAccess 1631
Diese Richtlinie wird verwendet 1632
Einzelheiten zu den Richtlinien 1632
Version der Richtlinie 1632
JSON-Richtliniendokument 1632
Weitere Informationen 1634
AWSCodeCommitFullAccess 1634
Diese Richtlinie wird verwendet 1634
Einzelheiten zu den Richtlinien 1634
Version der Richtlinie 1634
JSON-Richtliniendokument 1635
Weitere Informationen 1639

AWSCodeCommitPowerUser 1639
Diese Richtlinie wird verwendet 1640
Einzelheiten zu den Richtlinien 1640
Version der Richtlinie 1640
JSON-Richtliniendokument 1640
Weitere Informationen 1645
AWSCodeCommitReadOnly 1645
Diese Richtlinie wird verwendet 1645
Einzelheiten zu den Richtlinien 1645
Version der Richtlinie 1646
JSON-Richtliniendokument 1646
Weitere Informationen 1648
AWSCodeDeployDeployerAccess 1649
Diese Richtlinie wird verwendet 1649
Einzelheiten zu den Richtlinien 1649
Version der Richtlinie 1649
JSON-Richtliniendokument 1649
Weitere Informationen 1651
AWSCodeDeployFullAccess 1651
Diese Richtlinie wird verwendet 1651
Einzelheiten zu den Richtlinien 1651
Version der Richtlinie 1651
JSON-Richtliniendokument 1652
Weitere Informationen 1653
AWSCodeDeployReadOnlyAccess 1653
Diese Richtlinie wird verwendet 1654
Einzelheiten zu den Richtlinien 1654
Version der Richtlinie 1654
JSON-Richtliniendokument 1654
Weitere Informationen 1655
AWSCodeDeployRole 1655
Diese Richtlinie wird verwendet 1656
Einzelheiten zu den Richtlinien 1656
Version der Richtlinie 1656
JSON-Richtliniendokument 1656
Weitere Informationen 1657

AWSCodeDeployRoleForCloudFormation 1658
Diese Richtlinie wird verwendet 1658
Einzelheiten zu den Richtlinien 1658
Version der Richtlinie 1658
JSON-Richtliniendokument 1658
Weitere Informationen 1659
AWSCodeDeployRoleForECS 1659
Diese Richtlinie wird verwendet 1659
Einzelheiten zu den Richtlinien 1659
Version der Richtlinie 1660
JSON-Richtliniendokument 1660
Weitere Informationen 1661
AWSCodeDeployRoleForECSLimited 1661
Diese Richtlinie wird verwendet 1661
Einzelheiten zu den Richtlinien 1661
Version der Richtlinie 1662
JSON-Richtliniendokument 1662
Weitere Informationen 1663
AWSCodeDeployRoleForLambda 1664
Diese Richtlinie wird verwendet 1664
Einzelheiten zu den Richtlinien 1664
Version der Richtlinie 1664
JSON-Richtliniendokument 1664
Weitere Informationen 1666
AWSCodeDeployRoleForLambdaLimited 1666
Diese Richtlinie wird verwendet 1666
Einzelheiten zu den Richtlinien 1666
Version der Richtlinie 1666
JSON-Richtliniendokument 1667
Weitere Informationen 1668
AWSCodePipeline_FullAccess 1668
Diese Richtlinie wird verwendet 1668
Einzelheiten zu den Richtlinien 1668
Version der Richtlinie 1668
JSON-Richtliniendokument 1669
Weitere Informationen 1672

AWSCodePipeline_ReadOnlyAccess 1673
Diese Richtlinie wird verwendet 1673
Einzelheiten zu den Richtlinien 1673
Version der Richtlinie 1673
JSON-Richtliniendokument 1673
Weitere Informationen 1674
AWSCodePipelineApproverAccess 1675
Diese Richtlinie wird verwendet 1675
Einzelheiten zu den Richtlinien 1675
Version der Richtlinie 1675
JSON-Richtliniendokument 1675
Weitere Informationen 1676
AWSCodePipelineCustomActionAccess 1676
Diese Richtlinie wird verwendet 1676
Einzelheiten zu den Richtlinien 1676
Version der Richtlinie 1677
JSON-Richtliniendokument 1677
Weitere Informationen 1677
AWSCodeStarFullAccess 1678
Diese Richtlinie wird verwendet 1678
Einzelheiten zu den Richtlinien 1678
Version der Richtlinie 1678
JSON-Richtliniendokument 1678
Weitere Informationen 1679
AWSCodeStarNotificationsServiceRolePolicy 1679
Diese Richtlinie wird verwendet 1679
Einzelheiten der Richtlinie 1680
Version der Richtlinie 1680
JSON-Richtliniendokument 1680
Weitere Informationen 1681
AWSCodeStarServiceRole 1681
Diese Richtlinie wird verwendet 1682
Einzelheiten zu den Richtlinien 1682
Version der Richtlinie 1682
JSON-Richtliniendokument 1682
Weitere Informationen 1687

AWSCompromisedKeyQuarantine 1687
Diese Richtlinie wird verwendet 1687
Einzelheiten zu den Richtlinien 1687
Version der Richtlinie 1688
JSON-Richtliniendokument 1688
Weitere Informationen 1689
AWSCompromisedKeyQuarantineV2 1689
Diese Richtlinie wird verwendet 1689
Einzelheiten zu den Richtlinien 1690
Version der Richtlinie 1690
JSON-Richtliniendokument 1690
Weitere Informationen 1692
AWSConfigMultiAccountSetupPolicy 1692
Diese Richtlinie wird verwendet 1692
Einzelheiten der Richtlinie 1692
Version der Richtlinie 1693
JSON-Richtliniendokument 1693
Weitere Informationen 1695
AWSConfigRemediationServiceRolePolicy 1695
Diese Richtlinie wird verwendet 1695
Einzelheiten der Richtlinie 1695
Version der Richtlinie 1695
JSON-Richtliniendokument 1696
Weitere Informationen 1696
AWSConfigRoleForOrganizations 1696
Diese Richtlinie wird verwendet 1697
Einzelheiten zu den Richtlinien 1697
Version der Richtlinie 1697
JSON-Richtliniendokument 1697
Weitere Informationen 1698
AWSConfigRulesExecutionRole 1698
Diese Richtlinie wird verwendet 1698
Einzelheiten zu den Richtlinien 1698
Version der Richtlinie 1698
JSON-Richtliniendokument 1699
Weitere Informationen 1699

AWSConfigServiceRolePolicy 1699
Diese Richtlinie wird verwendet 1700
Einzelheiten der Richtlinie 1700
Version der Richtlinie 1700
JSON-Richtliniendokument 1700
Weitere Informationen 1732
AWSConfigUserAccess 1732
Diese Richtlinie wird verwendet 1732
Einzelheiten zu den Richtlinien 1732
Version der Richtlinie 1732
JSON-Richtliniendokument 1733
Weitere Informationen 1733
AWSConnector 1733
Diese Richtlinie wird verwendet 1734
Einzelheiten zu den Richtlinien 1734
Version der Richtlinie 1734
JSON-Richtliniendokument 1734
Weitere Informationen 1736
AWSControlTowerAccountServiceRolePolicy 1736
Diese Richtlinie wird verwendet 1736
Einzelheiten der Richtlinie 1737
Version der Richtlinie 1737
JSON-Richtliniendokument 1737
Weitere Informationen 1739
AWSControlTowerServiceRolePolicy 1739
Diese Richtlinie wird verwendet 1739
Einzelheiten zu den Richtlinien 1739
Version der Richtlinie 1739
JSON-Richtliniendokument 1740
Weitere Informationen 1744
AWSCostAndUsageReportAutomationPolicy 1744
Diese Richtlinie wird verwendet 1745
Einzelheiten zu den Richtlinien 1745
Version der Richtlinie 1745
JSON-Richtliniendokument 1745
Weitere Informationen 1746

AWSDataExchangeFullAccess 1746
Diese Richtlinie wird verwendet 1747
Einzelheiten zu den Richtlinien 1747
Version der Richtlinie 1747
JSON-Richtliniendokument 1747
Weitere Informationen 1751
AWSDataExchangeProviderFullAccess 1751
Diese Richtlinie wird verwendet 1751
Einzelheiten zu den Richtlinien 1751
Version der Richtlinie 1751
JSON-Richtliniendokument 1752
Weitere Informationen 1755
AWSDataExchangeReadOnly 1755
Diese Richtlinie wird verwendet 1756
Einzelheiten zu den Richtlinien 1756
Version der Richtlinie 1756
JSON-Richtliniendokument 1756
Weitere Informationen 1757
AWSDataExchangeSubscriberFullAccess 1757
Diese Richtlinie wird verwendet 1757
Einzelheiten zu den Richtlinien 1758
Version der Richtlinie 1758
JSON-Richtliniendokument 1758
Weitere Informationen 1760
AWSDataLifecycleManagerServiceRole 1760
Diese Richtlinie wird verwendet 1761
Einzelheiten zu den Richtlinien 1761
Version der Richtlinie 1761
JSON-Richtliniendokument 1761
Weitere Informationen 1762
AWSDataLifecycleManagerServiceRoleForAMIManagement 1763
Diese Richtlinie wird verwendet 1763
Einzelheiten zu den Richtlinien 1763
Version der Richtlinie 1763
JSON-Richtliniendokument 1763
Weitere Informationen 1765

AWSDataLifecycleManagerSSMFullAccess 1765
Diese Richtlinie wird verwendet 1765
Einzelheiten zu den Richtlinien 1765
Version der Richtlinie 1765
JSON-Richtliniendokument 1766
Weitere Informationen 1767
AWSDataPipeline_FullAccess 1767
Diese Richtlinie wird verwendet 1767
Einzelheiten zu den Richtlinien 1768
Version der Richtlinie 1768
JSON-Richtliniendokument 1768
Weitere Informationen 1769
AWSDataPipeline_PowerUser 1769
Diese Richtlinie wird verwendet 1769
Einzelheiten zu den Richtlinien 1769
Version der Richtlinie 1770
JSON-Richtliniendokument 1770
Weitere Informationen 1771
AWSDataSyncDiscoveryServiceRolePolicy 1771
Diese Richtlinie wird verwendet 1771
Einzelheiten der Richtlinie 1771
Version der Richtlinie 1771
JSON-Richtliniendokument 1772
Weitere Informationen 1773
AWSDataSyncFullAccess 1773
Diese Richtlinie wird verwendet 1773
Einzelheiten zu den Richtlinien 1773
Version der Richtlinie 1773
JSON-Richtliniendokument 1774
Weitere Informationen 1775
AWSDataSyncReadOnlyAccess 1775
Diese Richtlinie wird verwendet 1775
Einzelheiten zu den Richtlinien 1775
Version der Richtlinie 1776
JSON-Richtliniendokument 1776
Weitere Informationen 1776

AWSDeadlineCloud-FleetWorker 1777
Diese Richtlinie wird verwendet 1777
Einzelheiten zu den Richtlinien 1777
Version der Richtlinie 1777
JSON-Richtliniendokument 1777
Weitere Informationen 1778
AWSDeadlineCloud-UserAccessFarms 1778
Diese Richtlinie wird verwendet 1778
Einzelheiten zu den Richtlinien 1779
Version der Richtlinie 1779
JSON-Richtliniendokument 1779
Weitere Informationen 1784
AWSDeadlineCloud-UserAccessFleets 1785
Diese Richtlinie wird verwendet 1785
Einzelheiten zu den Richtlinien 1785
Version der Richtlinie 1785
JSON-Richtliniendokument 1785
Weitere Informationen 1789
AWSDeadlineCloud-UserAccessJobs 1789
Diese Richtlinie wird verwendet 1789
Einzelheiten zu den Richtlinien 1789
Version der Richtlinie 1790
JSON-Richtliniendokument 1790
Weitere Informationen 1794
AWSDeadlineCloud-UserAccessQueues 1794
Diese Richtlinie wird verwendet 1794
Einzelheiten zu den Richtlinien 1794
Version der Richtlinie 1794
JSON-Richtliniendokument 1795
Weitere Informationen 1799
AWSDeadlineCloud-WorkerHost 1800
Diese Richtlinie wird verwendet 1800
Einzelheiten zu den Richtlinien 1800
Version der Richtlinie 1800
JSON-Richtliniendokument 1800
Weitere Informationen 1801

AWSDeepLensLambdaFunctionAccessPolicy 1801
Diese Richtlinie wird verwendet 1801
Einzelheiten zu den Richtlinien 1801
Version der Richtlinie 1802
JSON-Richtliniendokument 1802
Weitere Informationen 1803
AWSDeepLensServiceRolePolicy 1803
Diese Richtlinie wird verwendet 1803
Einzelheiten zu den Richtlinien 1804
Version der Richtlinie 1804
JSON-Richtliniendokument 1804
Weitere Informationen 1811
AWSDeepRacerAccountAdminAccess 1811
Diese Richtlinie wird verwendet 1811
Einzelheiten zu den Richtlinien 1812
Version der Richtlinie 1812
JSON-Richtliniendokument 1812
Weitere Informationen 1813
AWSDeepRacerCloudFormationAccessPolicy 1813
Diese Richtlinie wird verwendet 1813
Einzelheiten zu den Richtlinien 1813
Version der Richtlinie 1813
JSON-Richtliniendokument 1814
Weitere Informationen 1816
AWSDeepRacerDefaultMultiUserAccess 1817
Diese Richtlinie wird verwendet 1817
Einzelheiten zu den Richtlinien 1817
Version der Richtlinie 1817
JSON-Richtliniendokument 1817
Weitere Informationen 1819
AWSDeepRacerFullAccess 1819
Diese Richtlinie wird verwendet 1819
Einzelheiten zu den Richtlinien 1819
Version der Richtlinie 1820
JSON-Richtliniendokument 1820
Weitere Informationen 1821

AWSDeepRacerRoboMakerAccessPolicy 1821
Diese Richtlinie wird verwendet 1821
Einzelheiten zu den Richtlinien 1821
Version der Richtlinie 1821
JSON-Richtliniendokument 1822
Weitere Informationen 1824
AWSDeepRacerServiceRolePolicy 1824
Diese Richtlinie wird verwendet 1824
Einzelheiten zu den Richtlinien 1824
Version der Richtlinie 1824
JSON-Richtliniendokument 1825
Weitere Informationen 1828
AWSDenyAll 1828
Diese Richtlinie wird verwendet 1828
Einzelheiten zu den Richtlinien 1828
Version der Richtlinie 1828
JSON-Richtliniendokument 1829
Weitere Informationen 1829
AWSDeviceFarmFullAccess 1829
Diese Richtlinie wird verwendet 1829
Einzelheiten zu den Richtlinien 1829
Version der Richtlinie 1830
JSON-Richtliniendokument 1830
Weitere Informationen 1830
AWSDeviceFarmServiceRolePolicy 1831
Diese Richtlinie wird verwendet 1831
Einzelheiten der Richtlinie 1831
Version der Richtlinie 1831
JSON-Richtliniendokument 1831
Weitere Informationen 1833
AWSDeviceFarmTestGridServiceRolePolicy 1834
Diese Richtlinie wird verwendet 1834
Einzelheiten der Richtlinie 1834
Version der Richtlinie 1834
JSON-Richtliniendokument 1834
Weitere Informationen 1836

AWSDirectConnectFullAccess 1837
Diese Richtlinie wird verwendet 1837
Einzelheiten zu den Richtlinien 1837
Version der Richtlinie 1837
JSON-Richtliniendokument 1837
Weitere Informationen 1838
AWSDirectConnectReadOnlyAccess 1838
Diese Richtlinie wird verwendet 1838
Einzelheiten zu den Richtlinien 1838
Version der Richtlinie 1838
JSON-Richtliniendokument 1839
Weitere Informationen 1839
AWSDirectConnectServiceRolePolicy 1839
Diese Richtlinie wird verwendet 1840
Einzelheiten der Richtlinie 1840
Version der Richtlinie 1840
JSON-Richtliniendokument 1840
Weitere Informationen 1841
AWSDirectoryServiceFullAccess 1841
Diese Richtlinie wird verwendet 1841
Einzelheiten zu den Richtlinien 1841
Version der Richtlinie 1841
JSON-Richtliniendokument 1842
Weitere Informationen 1843
AWSDirectoryServiceReadOnlyAccess 1844
Diese Richtlinie wird verwendet 1844
Einzelheiten zu den Richtlinien 1844
Version der Richtlinie 1844
JSON-Richtliniendokument 1844
Weitere Informationen 1845
AWSDiscoveryContinuousExportFirehosePolicy 1845
Diese Richtlinie wird verwendet 1845
Einzelheiten zu den Richtlinien 1845
Version der Richtlinie 1846
JSON-Richtliniendokument 1846
Weitere Informationen 1847

AWSDMSFleetAdvisorServiceRolePolicy 1847
Diese Richtlinie wird verwendet 1847
Einzelheiten der Richtlinie 1847
Version der Richtlinie 1848
JSON-Richtliniendokument 1848
Weitere Informationen 1848
AWSDMSServerlessServiceRolePolicy 1848
Diese Richtlinie wird verwendet 1849
Einzelheiten der Richtlinie 1849
Version der Richtlinie 1849
JSON-Richtliniendokument 1849
Weitere Informationen 1851
AWSEC2CapacityReservationFleetRolePolicy 1851
Diese Richtlinie wird verwendet 1851
Einzelheiten der Richtlinie 1851
Version der Richtlinie 1851
JSON-Richtliniendokument 1852
Weitere Informationen 1853
AWSEC2FleetServiceRolePolicy 1853
Diese Richtlinie wird verwendet 1853
Einzelheiten der Richtlinie 1853
Version der Richtlinie 1853
JSON-Richtliniendokument 1854
Weitere Informationen 1856
AWSEC2SpotFleetServiceRolePolicy 1856
Diese Richtlinie wird verwendet 1856
Einzelheiten der Richtlinie 1856
Version der Richtlinie 1856
JSON-Richtliniendokument 1857
Weitere Informationen 1858
AWSEC2SpotServiceRolePolicy 1859
Diese Richtlinie wird verwendet 1859
Einzelheiten der Richtlinie 1859
Version der Richtlinie 1859
JSON-Richtliniendokument 1859
Weitere Informationen 1861

AWSEC2VssSnapshotPolicy 1861
Diese Richtlinie wird verwendet 1861
Einzelheiten zu den Richtlinien 1861
Version der Richtlinie 1862
JSON-Richtliniendokument 1862
Weitere Informationen 1865
AWSECRPullThroughCache_ServiceRolePolicy 1865
Diese Richtlinie wird verwendet 1865
Einzelheiten der Richtlinie 1866
Version der Richtlinie 1866
JSON-Richtliniendokument 1866
Weitere Informationen 1867
AWSElasticBeanstalkCustomPlatformforEC2Role 1867
Diese Richtlinie wird verwendet 1867
Einzelheiten zu den Richtlinien 1867
Version der Richtlinie 1868
JSON-Richtliniendokument 1868
Weitere Informationen 1869
AWSElasticBeanstalkEnhancedHealth 1870
Diese Richtlinie wird verwendet 1870
Einzelheiten zu den Richtlinien 1870
Version der Richtlinie 1870
JSON-Richtliniendokument 1870
Weitere Informationen 1871
AWSElasticBeanstalkMaintenance 1872
Diese Richtlinie wird verwendet 1872
Einzelheiten der Richtlinie 1872
Version der Richtlinie 1872
JSON-Richtliniendokument 1872
Weitere Informationen 1873
AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 1873
Diese Richtlinie wird verwendet 1874
Einzelheiten zu den Richtlinien 1874
Version der Richtlinie 1874
JSON-Richtliniendokument 1874
Weitere Informationen 1881

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 1881
Diese Richtlinie wird verwendet 1881
Einzelheiten der Richtlinie 1881
Version der Richtlinie 1882
JSON-Richtliniendokument 1882
Weitere Informationen 1887
AWSElasticBeanstalkMulticontainerDocker 1887
Diese Richtlinie wird verwendet 1887
Einzelheiten zu den Richtlinien 1888
Version der Richtlinie 1888
JSON-Richtliniendokument 1888
Weitere Informationen 1889
AWSElasticBeanstalkReadOnly 1889
Diese Richtlinie wird verwendet 1889
Einzelheiten zu den Richtlinien 1890
Version der Richtlinie 1890
JSON-Richtliniendokument 1890
Weitere Informationen 1892
AWSElasticBeanstalkRoleCore 1892
Diese Richtlinie wird verwendet 1892
Einzelheiten zu den Richtlinien 1893
Version der Richtlinie 1893
JSON-Richtliniendokument 1893
Weitere Informationen 1898
AWSElasticBeanstalkRoleCWL 1898
Diese Richtlinie wird verwendet 1898
Einzelheiten zu den Richtlinien 1898
Version der Richtlinie 1899
JSON-Richtliniendokument 1899
Weitere Informationen 1899
AWSElasticBeanstalkRoleECS 1900
Diese Richtlinie wird verwendet 1900
Einzelheiten zu den Richtlinien 1900
Version der Richtlinie 1900
JSON-Richtliniendokument 1900
Weitere Informationen 1901

AWSElasticBeanstalkRoleRDS 1901
Diese Richtlinie wird verwendet 1902
Einzelheiten zu den Richtlinien 1902
Version der Richtlinie 1902
JSON-Richtliniendokument 1902
Weitere Informationen 1903
AWSElasticBeanstalkRoleSNS 1903
Diese Richtlinie wird verwendet 1903
Einzelheiten zu den Richtlinien 1903
Version der Richtlinie 1903
JSON-Richtliniendokument 1904
Weitere Informationen 1904
AWSElasticBeanstalkRoleWorkerTier 1905
Diese Richtlinie wird verwendet 1905
Einzelheiten zu den Richtlinien 1905
Version der Richtlinie 1905
JSON-Richtliniendokument 1905
Weitere Informationen 1906
AWSElasticBeanstalkService 1906
Diese Richtlinie wird verwendet 1907
Einzelheiten zu den Richtlinien 1907
Version der Richtlinie 1907
JSON-Richtliniendokument 1907
Weitere Informationen 1911
AWSElasticBeanstalkServiceRolePolicy 1912
Diese Richtlinie wird verwendet 1912
Einzelheiten der Richtlinie 1912
Version der Richtlinie 1912
JSON-Richtliniendokument 1912
Weitere Informationen 1914
AWSElasticBeanstalkWebTier 1914
Diese Richtlinie wird verwendet 1914
Einzelheiten zu den Richtlinien 1914
Version der Richtlinie 1914
JSON-Richtliniendokument 1915
Weitere Informationen 1916

AWSElasticBeanstalkWorkerTier 1916
Diese Richtlinie wird verwendet 1916
Einzelheiten zu den Richtlinien 1917
Version der Richtlinie 1917
JSON-Richtliniendokument 1917
Weitere Informationen 1919
AWSElasticDisasterRecoveryAgentInstallationPolicy 1919
Diese Richtlinie wird verwendet 1920
Einzelheiten zu den Richtlinien 1920
Version der Richtlinie 1920
JSON-Richtliniendokument 1920
Weitere Informationen 1922
AWSElasticDisasterRecoveryAgentPolicy 1922
Diese Richtlinie wird verwendet 1922
Einzelheiten zu den Richtlinien 1922
Version der Richtlinie 1922
JSON-Richtliniendokument 1923
Weitere Informationen 1923
AWSElasticDisasterRecoveryConsoleFullAccess 1924
Diese Richtlinie wird verwendet 1924
Einzelheiten zu den Richtlinien 1924
Version der Richtlinie 1924
JSON-Richtliniendokument 1924
Weitere Informationen 1934
AWSElasticDisasterRecoveryConsoleFullAccess_v2 1934
Diese Richtlinie wird verwendet 1935
Einzelheiten zu den Richtlinien 1935
Version der Richtlinie 1935
JSON-Richtliniendokument 1935
Weitere Informationen 1948
AWSElasticDisasterRecoveryConversionServerPolicy 1948
Diese Richtlinie wird verwendet 1948
Einzelheiten zu den Richtlinien 1948
Version der Richtlinie 1949
JSON-Richtliniendokument 1949
Weitere Informationen 1949

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 1950
Diese Richtlinie wird verwendet 1950
Einzelheiten zu den Richtlinien 1950
Version der Richtlinie 1950
JSON-Richtliniendokument 1951
Weitere Informationen 1951
AWSElasticDisasterRecoveryEc2InstancePolicy 1952
Diese Richtlinie wird verwendet 1952
Einzelheiten zu den Richtlinien 1952
Version der Richtlinie 1952
JSON-Richtliniendokument 1952
Weitere Informationen 1954
AWSElasticDisasterRecoveryFailbackInstallationPolicy 1955
Diese Richtlinie wird verwendet 1955
Einzelheiten zu den Richtlinien 1955
Version der Richtlinie 1955
JSON-Richtliniendokument 1955
Weitere Informationen 1956
AWSElasticDisasterRecoveryFailbackPolicy 1956
Diese Richtlinie wird verwendet 1957
Einzelheiten zu den Richtlinien 1957
Version der Richtlinie 1957
JSON-Richtliniendokument 1957
Weitere Informationen 1958
AWSElasticDisasterRecoveryLaunchActionsPolicy 1959
Diese Richtlinie wird verwendet 1959
Einzelheiten zu den Richtlinien 1959
Version der Richtlinie 1959
JSON-Richtliniendokument 1959
Weitere Informationen 1965
AWSElasticDisasterRecoveryNetworkReplicationPolicy 1966
Diese Richtlinie wird verwendet 1966
Einzelheiten zu den Richtlinien 1966
Version der Richtlinie 1966
JSON-Richtliniendokument 1966
Weitere Informationen 1967

AWSElasticDisasterRecoveryReadOnlyAccess 1967
Diese Richtlinie wird verwendet 1968
Einzelheiten zu den Richtlinien 1968
Version der Richtlinie 1968
JSON-Richtliniendokument 1968
Weitere Informationen 1970
AWSElasticDisasterRecoveryRecoveryInstancePolicy 1970
Diese Richtlinie wird verwendet 1971
Einzelheiten zu den Richtlinien 1971
Version der Richtlinie 1971
JSON-Richtliniendokument 1971
Weitere Informationen 1974
AWSElasticDisasterRecoveryReplicationServerPolicy 1974
Diese Richtlinie wird verwendet 1974
Einzelheiten zu den Richtlinien 1974
Version der Richtlinie 1975
JSON-Richtliniendokument 1975
Weitere Informationen 1977
AWSElasticDisasterRecoveryServiceRolePolicy 1977
Diese Richtlinie wird verwendet 1977
Einzelheiten der Richtlinie 1978
Version der Richtlinie 1978
JSON-Richtliniendokument 1978
Weitere Informationen 1986
AWSElasticDisasterRecoveryStagingAccountPolicy 1987
Diese Richtlinie wird verwendet 1987
Einzelheiten zu den Richtlinien 1987
Version der Richtlinie 1987
JSON-Richtliniendokument 1987
Weitere Informationen 1988
AWSElasticDisasterRecoveryStagingAccountPolicy_v2 1989
Diese Richtlinie wird verwendet 1989
Einzelheiten zu den Richtlinien 1989
Version der Richtlinie 1989
JSON-Richtliniendokument 1989
Weitere Informationen 1990

AWSElasticLoadBalancingClassicServiceRolePolicy 1991
Diese Richtlinie wird verwendet 1991
Einzelheiten der Richtlinie 1991
Version der Richtlinie 1991
JSON-Richtliniendokument 1991
Weitere Informationen 1992
AWSElasticLoadBalancingServiceRolePolicy 1992
Diese Richtlinie wird verwendet 1993
Einzelheiten der Richtlinie 1993
Version der Richtlinie 1993
JSON-Richtliniendokument 1993
Weitere Informationen 1994
AWSElementalMediaConvertFullAccess 1994
Diese Richtlinie wird verwendet 1995
Einzelheiten zu den Richtlinien 1995
Version der Richtlinie 1995
JSON-Richtliniendokument 1995
Weitere Informationen 1996
AWSElementalMediaConvertReadOnly 1996
Diese Richtlinie wird verwendet 1996
Einzelheiten zu den Richtlinien 1996
Version der Richtlinie 1997
JSON-Richtliniendokument 1997
Weitere Informationen 1997
AWSElementalMediaLiveFullAccess 1998
Diese Richtlinie wird verwendet 1998
Einzelheiten zu den Richtlinien 1998
Version der Richtlinie 1998
JSON-Richtliniendokument 1998
Weitere Informationen 1999
AWSElementalMediaLiveReadOnly 1999
Diese Richtlinie wird verwendet 1999
Einzelheiten zu den Richtlinien 1999
Version der Richtlinie 1999
JSON-Richtliniendokument 2000
Weitere Informationen 2000

AWSElementalMediaPackageFullAccess 2000
Diese Richtlinie wird verwendet 2000
Einzelheiten zu den Richtlinien 2000
Version der Richtlinie 2001
JSON-Richtliniendokument 2001
Weitere Informationen 2001
AWSElementalMediaPackageReadOnly 2001
Diese Richtlinie wird verwendet 2002
Einzelheiten zu den Richtlinien 2002
Version der Richtlinie 2002
JSON-Richtliniendokument 2002
Weitere Informationen 2002
AWSElementalMediaPackageV2FullAccess 2003
Diese Richtlinie wird verwendet 2003
Einzelheiten zu den Richtlinien 2003
Version der Richtlinie 2003
JSON-Richtliniendokument 2003
Weitere Informationen 2004
AWSElementalMediaPackageV2ReadOnly 2004
Diese Richtlinie wird verwendet 2004
Einzelheiten zu den Richtlinien 2004
Version der Richtlinie 2004
JSON-Richtliniendokument 2005
Weitere Informationen 2005
AWSElementalMediaStoreFullAccess 2005
Diese Richtlinie wird verwendet 2005
Einzelheiten zu den Richtlinien 2005
Version der Richtlinie 2006
JSON-Richtliniendokument 2006
Weitere Informationen 2006
AWSElementalMediaStoreReadOnly 2007
Diese Richtlinie wird verwendet 2007
Einzelheiten zu den Richtlinien 2007
Version der Richtlinie 2007
JSON-Richtliniendokument 2007
Weitere Informationen 2008

AWSElementalMediaTailorFullAccess 2008
Diese Richtlinie wird verwendet 2008
Einzelheiten zu den Richtlinien 2008
Version der Richtlinie 2009
JSON-Richtliniendokument 2009
Weitere Informationen 2009
AWSElementalMediaTailorReadOnly 2009
Diese Richtlinie wird verwendet 2009
Einzelheiten zu den Richtlinien 2010
Version der Richtlinie 2010
JSON-Richtliniendokument 2010
Weitere Informationen 2010
AWSEnhancedClassicNetworkingMangementPolicy 2011
Diese Richtlinie wird verwendet 2011
Einzelheiten der Richtlinie 2011
Version der Richtlinie 2011
JSON-Richtliniendokument 2011
Weitere Informationen 2012
AWSEntityResolutionConsoleFullAccess 2012
Diese Richtlinie wird verwendet 2012
Einzelheiten zu den Richtlinien 2012
Version der Richtlinie 2012
JSON-Richtliniendokument 2013
Weitere Informationen 2015
AWSEntityResolutionConsoleReadOnlyAccess 2016
Diese Richtlinie wird verwendet 2016
Einzelheiten zu den Richtlinien 2016
Version der Richtlinie 2016
JSON-Richtliniendokument 2016
Weitere Informationen 2017
AWSFaultInjectionSimulatorEC2Access 2017
Diese Richtlinie wird verwendet 2017
Einzelheiten zu den Richtlinien 2017
Version der Richtlinie 2017
JSON-Richtliniendokument 2018
Weitere Informationen 2019

AWSFaultInjectionSimulatorECSAccess 2019
Diese Richtlinie wird verwendet 2020
Einzelheiten zu den Richtlinien 2020
Version der Richtlinie 2020
JSON-Richtliniendokument 2020
Weitere Informationen 2022
AWSFaultInjectionSimulatorEKSAccess 2022
Diese Richtlinie wird verwendet 2022
Einzelheiten zu den Richtlinien 2022
Version der Richtlinie 2023
JSON-Richtliniendokument 2023
Weitere Informationen 2024
AWSFaultInjectionSimulatorNetworkAccess 2024
Diese Richtlinie wird verwendet 2024
Einzelheiten zu den Richtlinien 2024
Version der Richtlinie 2025
JSON-Richtliniendokument 2025
Weitere Informationen 2032
AWSFaultInjectionSimulatorRDSAccess 2032
Diese Richtlinie wird verwendet 2032
Einzelheiten zu den Richtlinien 2032
Version der Richtlinie 2033
JSON-Richtliniendokument 2033
Weitere Informationen 2034
AWSFaultInjectionSimulatorSSMAccess 2034
Diese Richtlinie wird verwendet 2034
Einzelheiten zu den Richtlinien 2034
Version der Richtlinie 2035
JSON-Richtliniendokument 2035
Weitere Informationen 2036
AWSFinSpaceServiceRolePolicy 2036
Diese Richtlinie wird verwendet 2036
Einzelheiten der Richtlinie 2037
Version der Richtlinie 2037
JSON-Richtliniendokument 2037
Weitere Informationen 2038

AWSFMAdminFullAccess 2038
Diese Richtlinie wird verwendet 2038
Einzelheiten zu den Richtlinien 2038
Version der Richtlinie 2038
JSON-Richtliniendokument 2038
Weitere Informationen 2040
AWSFMAdminReadOnlyAccess 2041
Diese Richtlinie wird verwendet 2041
Einzelheiten zu den Richtlinien 2041
Version der Richtlinie 2041
JSON-Richtliniendokument 2041
Weitere Informationen 2043
AWSFMMemberReadOnlyAccess 2043
Diese Richtlinie wird verwendet 2043
Einzelheiten zu den Richtlinien 2043
Version der Richtlinie 2043
JSON-Richtliniendokument 2044
Weitere Informationen 2044
AWSForWordPressPluginPolicy 2044
Diese Richtlinie wird verwendet 2045
Einzelheiten zu den Richtlinien 2045
Version der Richtlinie 2045
JSON-Richtliniendokument 2045
Weitere Informationen 2047
AWSGitSyncServiceRolePolicy 2047
Diese Richtlinie wird verwendet 2047
Einzelheiten der Richtlinie 2047
Version der Richtlinie 2048
JSON-Richtliniendokument 2048
Weitere Informationen 2048
AWSGlobalAcceleratorSLRPolicy 2049
Diese Richtlinie wird verwendet 2049
Einzelheiten der Richtlinie 2049
Version der Richtlinie 2049
JSON-Richtliniendokument 2049
Weitere Informationen 2051

AWSGlueConsoleFullAccess 2051
Diese Richtlinie wird verwendet 2051
Einzelheiten zu den Richtlinien 2051
Version der Richtlinie 2052
JSON-Richtliniendokument 2052
Weitere Informationen 2056
AWSGlueConsoleSageMakerNotebookFullAccess 2056
Diese Richtlinie wird verwendet 2056
Einzelheiten zu den Richtlinien 2056
Version der Richtlinie 2057
JSON-Richtliniendokument 2057
Weitere Informationen 2062
AwsGlueDataBrewFullAccessPolicy 2062
Diese Richtlinie wird verwendet 2062
Einzelheiten zu den Richtlinien 2063
Version der Richtlinie 2063
JSON-Richtliniendokument 2063
Weitere Informationen 2068
AWSGlueDataBrewServiceRole 2068
Diese Richtlinie wird verwendet 2069
Einzelheiten zu den Richtlinien 2069
Version der Richtlinie 2069
JSON-Richtliniendokument 2069
Weitere Informationen 2072
AWSGlueSchemaRegistryFullAccess 2072
Diese Richtlinie wird verwendet 2072
Einzelheiten zu den Richtlinien 2072
Version der Richtlinie 2073
JSON-Richtliniendokument 2073
Weitere Informationen 2074
AWSGlueSchemaRegistryReadonlyAccess 2074
Diese Richtlinie wird verwendet 2074
Einzelheiten zu den Richtlinien 2074
Version der Richtlinie 2075
JSON-Richtliniendokument 2075
Weitere Informationen 2076

AWSGlueServiceNotebookRole 2076
Diese Richtlinie wird verwendet 2076
Einzelheiten zu den Richtlinien 2076
Version der Richtlinie 2076
JSON-Richtliniendokument 2077
Weitere Informationen 2079
AWSGlueServiceRole 2079
Diese Richtlinie wird verwendet 2079
Einzelheiten zu den Richtlinien 2079
Version der Richtlinie 2080
JSON-Richtliniendokument 2080
Weitere Informationen 2082
AwsGlueSessionUserRestrictedNotebookPolicy 2082
Diese Richtlinie wird verwendet 2082
Einzelheiten zu den Richtlinien 2083
Version der Richtlinie 2083
JSON-Richtliniendokument 2083
Weitere Informationen 2085
AwsGlueSessionUserRestrictedNotebookServiceRole 2086
Diese Richtlinie wird verwendet 2086
Einzelheiten zu den Richtlinien 2086
Version der Richtlinie 2086
JSON-Richtliniendokument 2087
Weitere Informationen 2090
AwsGlueSessionUserRestrictedPolicy 2090
Diese Richtlinie wird verwendet 2091
Einzelheiten zu den Richtlinien 2091
Version der Richtlinie 2091
JSON-Richtliniendokument 2091
Weitere Informationen 2094
AwsGlueSessionUserRestrictedServiceRole 2094
Diese Richtlinie wird verwendet 2094
Einzelheiten zu den Richtlinien 2094
Version der Richtlinie 2094
JSON-Richtliniendokument 2095
Weitere Informationen 2099

AWSGrafanaAccountAdministrator 2099
Diese Richtlinie wird verwendet 2099
Einzelheiten zu den Richtlinien 2099
Version der Richtlinie 2099
JSON-Richtliniendokument 2100
Weitere Informationen 2101
AWSGrafanaConsoleReadOnlyAccess 2101
Diese Richtlinie wird verwendet 2101
Einzelheiten zu den Richtlinien 2101
Version der Richtlinie 2101
JSON-Richtliniendokument 2102
Weitere Informationen 2102
AWSGrafanaWorkspacePermissionManagement 2102
Diese Richtlinie wird verwendet 2102
Einzelheiten zu den Richtlinien 2103
Version der Richtlinie 2103
JSON-Richtliniendokument 2103
Weitere Informationen 2104
AWSGrafanaWorkspacePermissionManagementV2 2104
Diese Richtlinie wird verwendet 2104
Einzelheiten zu den Richtlinien 2104
Version der Richtlinie 2105
JSON-Richtliniendokument 2105
Weitere Informationen 2106
AWSGreengrassFullAccess 2106
Diese Richtlinie wird verwendet 2106
Einzelheiten zu den Richtlinien 2106
Version der Richtlinie 2106
JSON-Richtliniendokument 2107
Weitere Informationen 2107
AWSGreengrassReadOnlyAccess 2107
Diese Richtlinie wird verwendet 2107
Einzelheiten zu den Richtlinien 2108
Version der Richtlinie 2108
JSON-Richtliniendokument 2108
Weitere Informationen 2108

AWSGreengrassResourceAccessRolePolicy 2109
Diese Richtlinie wird verwendet 2109
Einzelheiten zu den Richtlinien 2109
Version der Richtlinie 2109
JSON-Richtliniendokument 2109
Weitere Informationen 2112
AWSGroundStationAgentInstancePolicy 2112
Diese Richtlinie wird verwendet 2112
Einzelheiten zu den Richtlinien 2112
Version der Richtlinie 2112
JSON-Richtliniendokument 2113
Weitere Informationen 2113
AWSHealth_EventProcessorServiceRolePolicy 2113
Diese Richtlinie wird verwendet 2113
Einzelheiten der Richtlinie 2114
Version der Richtlinie 2114
JSON-Richtliniendokument 2114
Weitere Informationen 2115
AWSHealthFullAccess 2115
Diese Richtlinie wird verwendet 2115
Einzelheiten zu den Richtlinien 2115
Version der Richtlinie 2115
JSON-Richtliniendokument 2116
Weitere Informationen 2117
AWSHealthImagingFullAccess 2117
Diese Richtlinie wird verwendet 2117
Einzelheiten zu den Richtlinien 2117
Version der Richtlinie 2117
JSON-Richtliniendokument 2118
Weitere Informationen 2118
AWSHealthImagingReadOnlyAccess 2118
Diese Richtlinie wird verwendet 2119
Einzelheiten zu den Richtlinien 2119
Version der Richtlinie 2119
JSON-Richtliniendokument 2119
Weitere Informationen 2120

AWSIAMIdentityCenterAllowListForIdentityContext 2120
Diese Richtlinie wird verwendet 2120
Einzelheiten zu den Richtlinien 2120
Version der Richtlinie 2121
JSON-Richtliniendokument 2121
Weitere Informationen 2123
AWSIdentitySyncFullAccess 2124
Diese Richtlinie wird verwendet 2124
Einzelheiten zu den Richtlinien 2124
Version der Richtlinie 2124
JSON-Richtliniendokument 2124
Weitere Informationen 2125
AWSIdentitySyncReadOnlyAccess 2125
Diese Richtlinie wird verwendet 2126
Einzelheiten zu den Richtlinien 2126
Version der Richtlinie 2126
JSON-Richtliniendokument 2126
Weitere Informationen 2127
AWSImageBuilderFullAccess 2127
Diese Richtlinie wird verwendet 2127
Einzelheiten zu den Richtlinien 2127
Version der Richtlinie 2127
JSON-Richtliniendokument 2128
Weitere Informationen 2130
AWSImageBuilderReadOnlyAccess 2130
Diese Richtlinie wird verwendet 2131
Einzelheiten zu den Richtlinien 2131
Version der Richtlinie 2131
JSON-Richtliniendokument 2131
Weitere Informationen 2132
AWSImportExportFullAccess 2132
Diese Richtlinie wird verwendet 2132
Einzelheiten zu den Richtlinien 2132
Version der Richtlinie 2132
JSON-Richtliniendokument 2133
Weitere Informationen 2133

AWSImportExportReadOnlyAccess 2133
Diese Richtlinie wird verwendet 2133
Einzelheiten zu den Richtlinien 2134
Version der Richtlinie 2134
JSON-Richtliniendokument 2134
Weitere Informationen 2134
AWSIncidentManagerIncidentAccessServiceRolePolicy 2135
Diese Richtlinie wird verwendet 2135
Einzelheiten zu den Richtlinien 2135
Version der Richtlinie 2135
JSON-Richtliniendokument 2135
Weitere Informationen 2136
AWSIncidentManagerResolverAccess 2136
Diese Richtlinie wird verwendet 2136
Einzelheiten zu den Richtlinien 2136
Version der Richtlinie 2137
JSON-Richtliniendokument 2137
Weitere Informationen 2138
AWSIncidentManagerServiceRolePolicy 2138
Diese Richtlinie wird verwendet 2138
Einzelheiten der Richtlinie 2138
Version der Richtlinie 2139
JSON-Richtliniendokument 2139
Weitere Informationen 2140
AWSIoT1ClickFullAccess 2140
Diese Richtlinie wird verwendet 2140
Einzelheiten zu den Richtlinien 2140
Version der Richtlinie 2141
JSON-Richtliniendokument 2141
Weitere Informationen 2141
AWSIoT1ClickReadOnlyAccess 2141
Diese Richtlinie wird verwendet 2142
Einzelheiten zu den Richtlinien 2142
Version der Richtlinie 2142
JSON-Richtliniendokument 2142
Weitere Informationen 2143

AWSIoTAnalyticsFullAccess 2143
Diese Richtlinie wird verwendet 2143
Einzelheiten zu den Richtlinien 2143
Version der Richtlinie 2143
JSON-Richtliniendokument 2144
Weitere Informationen 2144
AWSIoTAnalyticsReadOnlyAccess 2144
Diese Richtlinie wird verwendet 2144
Einzelheiten zu den Richtlinien 2144
Version der Richtlinie 2145
JSON-Richtliniendokument 2145
Weitere Informationen 2145
AWSIoTConfigAccess 2146
Diese Richtlinie wird verwendet 2146
Einzelheiten zu den Richtlinien 2146
Version der Richtlinie 2146
JSON-Richtliniendokument 2146
Weitere Informationen 2150
AWSIoTConfigReadOnlyAccess 2150
Diese Richtlinie wird verwendet 2150
Einzelheiten zu den Richtlinien 2151
Version der Richtlinie 2151
JSON-Richtliniendokument 2151
Weitere Informationen 2153
AWSIoTDataAccess 2153
Diese Richtlinie wird verwendet 2153
Einzelheiten zu den Richtlinien 2153
Version der Richtlinie 2154
JSON-Richtliniendokument 2154
Weitere Informationen 2154
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 2155
Diese Richtlinie wird verwendet 2155
Einzelheiten zu den Richtlinien 2155
Version der Richtlinie 2155
JSON-Richtliniendokument 2155
Weitere Informationen 2156

AWSIoTDeviceDefenderAudit 2156
Diese Richtlinie wird verwendet 2156
Einzelheiten zu den Richtlinien 2156
Version der Richtlinie 2157
JSON-Richtliniendokument 2157
Weitere Informationen 2158
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 2158
Diese Richtlinie wird verwendet 2158
Einzelheiten zu den Richtlinien 2158
Version der Richtlinie 2158
JSON-Richtliniendokument 2159
Weitere Informationen 2159
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 2160
Diese Richtlinie wird verwendet 2160
Einzelheiten zu den Richtlinien 2160
Version der Richtlinie 2160
JSON-Richtliniendokument 2160
Weitere Informationen 2161
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 2161
Diese Richtlinie wird verwendet 2161
Einzelheiten zu den Richtlinien 2161
Version der Richtlinie 2162
JSON-Richtliniendokument 2162
Weitere Informationen 2162
AWSIoTDeviceDefenderUpdateCACertMitigationAction 2163
Diese Richtlinie wird verwendet 2163
Einzelheiten zu den Richtlinien 2163
Version der Richtlinie 2163
JSON-Richtliniendokument 2163
Weitere Informationen 2164
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 2164
Diese Richtlinie wird verwendet 2164
Einzelheiten zu den Richtlinien 2164
Version der Richtlinie 2165
JSON-Richtliniendokument 2165
Weitere Informationen 2165

AWSIoTDeviceTesterForFreeRTOSFullAccess 2165
Diese Richtlinie wird verwendet 2166
Einzelheiten zu den Richtlinien 2166
Version der Richtlinie 2166
JSON-Richtliniendokument 2166
Weitere Informationen 2172
AWSIoTDeviceTesterForGreengrassFullAccess 2173
Diese Richtlinie wird verwendet 2173
Einzelheiten zu den Richtlinien 2173
Version der Richtlinie 2173
JSON-Richtliniendokument 2173
Weitere Informationen 2176
AWSIoTEventsFullAccess 2176
Diese Richtlinie wird verwendet 2177
Einzelheiten zu den Richtlinien 2177
Version der Richtlinie 2177
JSON-Richtliniendokument 2177
Weitere Informationen 2177
AWSIoTEventsReadOnlyAccess 2178
Diese Richtlinie wird verwendet 2178
Einzelheiten zu den Richtlinien 2178
Version der Richtlinie 2178
JSON-Richtliniendokument 2178
Weitere Informationen 2179
AWSIoTFleetHubFederationAccess 2179
Diese Richtlinie wird verwendet 2179
Einzelheiten zu den Richtlinien 2179
Version der Richtlinie 2180
JSON-Richtliniendokument 2180
Weitere Informationen 2181
AWSIoTFleetwiseServiceRolePolicy 2182
Diese Richtlinie wird verwendet 2182
Einzelheiten der Richtlinie 2182
Version der Richtlinie 2182
JSON-Richtliniendokument 2183
Weitere Informationen 2183

AWSIoTFullAccess 2183
Diese Richtlinie wird verwendet 2183
Einzelheiten zu den Richtlinien 2184
Version der Richtlinie 2184
JSON-Richtliniendokument 2184
Weitere Informationen 2184
AWSIoTLogging 2185
Diese Richtlinie wird verwendet 2185
Einzelheiten zu den Richtlinien 2185
Version der Richtlinie 2185
JSON-Richtliniendokument 2185
Weitere Informationen 2186
AWSIoTOTAUpdate 2186
Diese Richtlinie wird verwendet 2186
Einzelheiten zu den Richtlinien 2186
Version der Richtlinie 2187
JSON-Richtliniendokument 2187
Weitere Informationen 2187
AWSIotRoboRunnerFullAccess 2187
Diese Richtlinie wird verwendet 2188
Einzelheiten zu den Richtlinien 2188
Version der Richtlinie 2188
JSON-Richtliniendokument 2188
Weitere Informationen 2189
AWSIotRoboRunnerReadOnly 2189
Diese Richtlinie wird verwendet 2189
Einzelheiten zu den Richtlinien 2189
Version der Richtlinie 2189
JSON-Richtliniendokument 2190
Weitere Informationen 2190
AWSIotRoboRunnerServiceRolePolicy 2190
Diese Richtlinie wird verwendet 2191
Einzelheiten der Richtlinie 2191
Version der Richtlinie 2191
JSON-Richtliniendokument 2191
Weitere Informationen 2192

AWSIoTRuleActions 2192
Diese Richtlinie wird verwendet 2192
Einzelheiten zu den Richtlinien 2192
Version der Richtlinie 2192
JSON-Richtliniendokument 2193
Weitere Informationen 2193
AWSIoTSiteWiseConsoleFullAccess 2193
Diese Richtlinie wird verwendet 2194
Einzelheiten zu den Richtlinien 2194
Version der Richtlinie 2194
JSON-Richtliniendokument 2194
Weitere Informationen 2196
AWSIoTSiteWiseFullAccess 2197
Diese Richtlinie wird verwendet 2197
Einzelheiten zu den Richtlinien 2197
Version der Richtlinie 2197
JSON-Richtliniendokument 2197
Weitere Informationen 2198
AWSIoTSiteWiseMonitorPortalAccess 2198
Diese Richtlinie wird verwendet 2198
Einzelheiten zu den Richtlinien 2198
Version der Richtlinie 2198
JSON-Richtliniendokument 2199
Weitere Informationen 2200
AWSIoTSiteWiseMonitorServiceRolePolicy 2200
Diese Richtlinie wird verwendet 2200
Einzelheiten der Richtlinie 2200
Version der Richtlinie 2200
JSON-Richtliniendokument 2201
Weitere Informationen 2202
AWSIoTSiteWiseReadOnlyAccess 2202
Diese Richtlinie wird verwendet 2202
Einzelheiten zu den Richtlinien 2202
Version der Richtlinie 2202
JSON-Richtliniendokument 2202
Weitere Informationen 2203

AWSIoTThingsRegistration 2203
Diese Richtlinie wird verwendet 2203
Einzelheiten zu den Richtlinien 2203
Version der Richtlinie 2204
JSON-Richtliniendokument 2204
Weitere Informationen 2205
AWSIoTTwinMakerServiceRolePolicy 2205
Diese Richtlinie wird verwendet 2205
Einzelheiten der Richtlinie 2206
Version der Richtlinie 2206
JSON-Richtliniendokument 2206
Weitere Informationen 2208
AWSIoTWirelessDataAccess 2208
Diese Richtlinie wird verwendet 2208
Einzelheiten zu den Richtlinien 2208
Version der Richtlinie 2208
JSON-Richtliniendokument 2208
Weitere Informationen 2209
AWSIoTWirelessFullAccess 2209
Diese Richtlinie wird verwendet 2209
Einzelheiten zu den Richtlinien 2209
Version der Richtlinie 2210
JSON-Richtliniendokument 2210
Weitere Informationen 2210
AWSIoTWirelessFullPublishAccess 2210
Diese Richtlinie wird verwendet 2211
Einzelheiten zu den Richtlinien 2211
Version der Richtlinie 2211
JSON-Richtliniendokument 2211
Weitere Informationen 2212
AWSIoTWirelessGatewayCertManager 2212
Diese Richtlinie wird verwendet 2212
Einzelheiten zu den Richtlinien 2212
Version der Richtlinie 2212
JSON-Richtliniendokument 2213
Weitere Informationen 2213

AWSIoTWirelessLogging 2213
Diese Richtlinie wird verwendet 2213
Einzelheiten zu den Richtlinien 2214
Version der Richtlinie 2214
JSON-Richtliniendokument 2214
Weitere Informationen 2214
AWSIoTWirelessReadOnlyAccess 2215
Diese Richtlinie wird verwendet 2215
Einzelheiten zu den Richtlinien 2215
Version der Richtlinie 2215
JSON-Richtliniendokument 2215
Weitere Informationen 2216
AWSIPAMServiceRolePolicy 2216
Diese Richtlinie wird verwendet 2216
Einzelheiten der Richtlinie 2216
Version der Richtlinie 2217
JSON-Richtliniendokument 2217
Weitere Informationen 2218
AWSIQContractServiceRolePolicy 2218
Diese Richtlinie wird verwendet 2218
Einzelheiten der Richtlinie 2218
Version der Richtlinie 2219
JSON-Richtliniendokument 2219
Weitere Informationen 2219
AWSIQFullAccess 2219
Diese Richtlinie wird verwendet 2220
Einzelheiten zu den Richtlinien 2220
Version der Richtlinie 2220
JSON-Richtliniendokument 2220
Weitere Informationen 2221
AWSIQPermissionServiceRolePolicy 2221
Diese Richtlinie wird verwendet 2221
Einzelheiten der Richtlinie 2221
Version der Richtlinie 2222
JSON-Richtliniendokument 2222
Weitere Informationen 2223

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2223
Diese Richtlinie wird verwendet 2223
Einzelheiten der Richtlinie 2223
Version der Richtlinie 2223
JSON-Richtliniendokument 2224
Weitere Informationen 2224
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2224
Diese Richtlinie wird verwendet 2225
Einzelheiten der Richtlinie 2225
Version der Richtlinie 2225
JSON-Richtliniendokument 2225
Weitere Informationen 2226
AWSKeyManagementServicePowerUser 2226
Diese Richtlinie wird verwendet 2226
Einzelheiten zu den Richtlinien 2226
Version der Richtlinie 2226
JSON-Richtliniendokument 2226
Weitere Informationen 2227
AWSLakeFormationCrossAccountManager 2227
Diese Richtlinie wird verwendet 2228
Einzelheiten zu den Richtlinien 2228
Version der Richtlinie 2228
JSON-Richtliniendokument 2228
Weitere Informationen 2230
AWSLakeFormationDataAdmin 2230
Diese Richtlinie wird verwendet 2230
Einzelheiten zu den Richtlinien 2231
Version der Richtlinie 2231
JSON-Richtliniendokument 2231
Weitere Informationen 2232
AWSLambda_FullAccess 2233
Diese Richtlinie wird verwendet 2233
Einzelheiten zu den Richtlinien 2233
Version der Richtlinie 2233
JSON-Richtliniendokument 2233
Weitere Informationen 2235

AWSLambda_ReadOnlyAccess 2235
Diese Richtlinie wird verwendet 2235
Einzelheiten zu den Richtlinien 2235
Version der Richtlinie 2235
JSON-Richtliniendokument 2236
Weitere Informationen 2237
AWSLambdaBasicExecutionRole 2237
Diese Richtlinie wird verwendet 2237
Einzelheiten zu den Richtlinien 2237
Version der Richtlinie 2238
JSON-Richtliniendokument 2238
Weitere Informationen 2238
AWSLambdaDynamoDBExecutionRole 2238
Diese Richtlinie wird verwendet 2239
Einzelheiten zu den Richtlinien 2239
Version der Richtlinie 2239
JSON-Richtliniendokument 2239
Weitere Informationen 2240
AWSLambdaENIManagementAccess 2240
Diese Richtlinie wird verwendet 2240
Einzelheiten zu den Richtlinien 2240
Version der Richtlinie 2240
JSON-Richtliniendokument 2241
Weitere Informationen 2241
AWSLambdaExecute 2241
Diese Richtlinie wird verwendet 2242
Einzelheiten zu den Richtlinien 2242
Version der Richtlinie 2242
JSON-Richtliniendokument 2242
Weitere Informationen 2243
AWSLambdaFullAccess 2243
Diese Richtlinie wird verwendet 2243
Einzelheiten zu den Richtlinien 2243
Version der Richtlinie 2243
JSON-Richtliniendokument 2244
Weitere Informationen 2245

AWSLambdaInvocation-DynamoDB 2245
Diese Richtlinie wird verwendet 2246
Einzelheiten zu den Richtlinien 2246
Version der Richtlinie 2246
JSON-Richtliniendokument 2246
Weitere Informationen 2247
AWSLambdaKinesisExecutionRole 2247
Diese Richtlinie wird verwendet 2247
Einzelheiten zu den Richtlinien 2247
Version der Richtlinie 2247
JSON-Richtliniendokument 2248
Weitere Informationen 2248
AWSLambdaMSKExecutionRole 2249
Diese Richtlinie wird verwendet 2249
Einzelheiten zu den Richtlinien 2249
Version der Richtlinie 2249
JSON-Richtliniendokument 2249
Weitere Informationen 2250
AWSLambdaReplicator 2250
Diese Richtlinie wird verwendet 2250
Einzelheiten der Richtlinie 2250
Version der Richtlinie 2251
JSON-Richtliniendokument 2251
Weitere Informationen 2252
AWSLambdaRole 2252
Diese Richtlinie wird verwendet 2252
Einzelheiten zu den Richtlinien 2252
Version der Richtlinie 2253
JSON-Richtliniendokument 2253
Weitere Informationen 2253
AWSLambdaSQSQueueExecutionRole 2253
Diese Richtlinie wird verwendet 2254
Einzelheiten zu den Richtlinien 2254
Version der Richtlinie 2254
JSON-Richtliniendokument 2254
Weitere Informationen 2255

AWSLambdaVPCAccessExecutionRole 2255
Diese Richtlinie wird verwendet 2255
Einzelheiten zu den Richtlinien 2255
Version der Richtlinie 2255
JSON-Richtliniendokument 2256
Weitere Informationen 2256
AWSLicenseManagerConsumptionPolicy 2256
Diese Richtlinie wird verwendet 2257
Einzelheiten zu den Richtlinien 2257
Version der Richtlinie 2257
JSON-Richtliniendokument 2257
Weitere Informationen 2258
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 2258
Diese Richtlinie wird verwendet 2258
Einzelheiten der Richtlinie 2258
Version der Richtlinie 2258
JSON-Richtliniendokument 2259
Weitere Informationen 2260
AWSLicenseManagerMasterAccountRolePolicy 2260
Diese Richtlinie wird verwendet 2260
Einzelheiten der Richtlinie 2260
Version der Richtlinie 2260
JSON-Richtliniendokument 2261
Weitere Informationen 2265
AWSLicenseManagerMemberAccountRolePolicy 2266
Diese Richtlinie wird verwendet 2266
Einzelheiten der Richtlinie 2266
Version der Richtlinie 2266
JSON-Richtliniendokument 2266
Weitere Informationen 2267
AWSLicenseManagerServiceRolePolicy 2268
Diese Richtlinie wird verwendet 2268
Einzelheiten der Richtlinie 2268
Version der Richtlinie 2268
JSON-Richtliniendokument 2268
Weitere Informationen 2272

AWSLicenseManagerUserSubscriptionsServiceRolePolicy 2272
Diese Richtlinie wird verwendet 2272
Einzelheiten der Richtlinie 2272
Version der Richtlinie 2272
JSON-Richtliniendokument 2273
Weitere Informationen 2274
AWSM2ServicePolicy 2275
Diese Richtlinie wird verwendet 2275
Einzelheiten der Richtlinie 2275
Version der Richtlinie 2275
JSON-Richtliniendokument 2275
Weitere Informationen 2277
AWSManagedServices_ContactsServiceRolePolicy 2277
Diese Richtlinie wird verwendet 2277
Einzelheiten der Richtlinie 2277
Version der Richtlinie 2277
JSON-Richtliniendokument 2278
Weitere Informationen 2278
AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 2279
Diese Richtlinie wird verwendet 2279
Einzelheiten der Richtlinie 2279
Version der Richtlinie 2279
JSON-Richtliniendokument 2279
Weitere Informationen 2281
AWSManagedServices_EventsServiceRolePolicy 2281
Diese Richtlinie wird verwendet 2281
Einzelheiten der Richtlinie 2281
Version der Richtlinie 2282
JSON-Richtliniendokument 2282
Weitere Informationen 2283
AWSManagedServicesDeploymentToolkitPolicy 2283
Diese Richtlinie wird verwendet 2283
Einzelheiten der Richtlinie 2283
Version der Richtlinie 2283
JSON-Richtliniendokument 2284
Weitere Informationen 2286

AWSMarketplaceAmiIngestion 2286
Diese Richtlinie wird verwendet 2286
Einzelheiten zu den Richtlinien 2286
Version der Richtlinie 2286
JSON-Richtliniendokument 2287
Weitere Informationen 2287
AWSMarketplaceDeploymentServiceRolePolicy 2287
Diese Richtlinie wird verwendet 2288
Einzelheiten der Richtlinie 2288
Version der Richtlinie 2288
JSON-Richtliniendokument 2288
Weitere Informationen 2290
AWSMarketplaceFullAccess 2290
Diese Richtlinie wird verwendet 2290
Einzelheiten zu den Richtlinien 2290
Version der Richtlinie 2290
JSON-Richtliniendokument 2291
Weitere Informationen 2294
AWSMarketplaceGetEntitlements 2294
Diese Richtlinie wird verwendet 2294
Einzelheiten zu den Richtlinien 2294
Version der Richtlinie 2294
JSON-Richtliniendokument 2295
Weitere Informationen 2295
AWSMarketplaceImageBuildFullAccess 2295
Diese Richtlinie wird verwendet 2295
Einzelheiten zu den Richtlinien 2296
Version der Richtlinie 2296
JSON-Richtliniendokument 2296
Weitere Informationen 2299
AWSMarketplaceLicenseManagementServiceRolePolicy 2300
Diese Richtlinie wird verwendet 2300
Einzelheiten der Richtlinie 2300
Version der Richtlinie 2300
JSON-Richtliniendokument 2301
Weitere Informationen 2301

AWSMarketplaceManageSubscriptions 2301
Diese Richtlinie wird verwendet 2302
Einzelheiten zu den Richtlinien 2302
Version der Richtlinie 2302
JSON-Richtliniendokument 2302
Weitere Informationen 2303
AWSMarketplaceMeteringFullAccess 2303
Diese Richtlinie wird verwendet 2303
Einzelheiten zu den Richtlinien 2303
Version der Richtlinie 2304
JSON-Richtliniendokument 2304
Weitere Informationen 2304
AWSMarketplaceMeteringRegisterUsage 2304
Diese Richtlinie wird verwendet 2305
Einzelheiten zu den Richtlinien 2305
Version der Richtlinie 2305
JSON-Richtliniendokument 2305
Weitere Informationen 2305
AWSMarketplaceProcurementSystemAdminFullAccess 2306
Diese Richtlinie wird verwendet 2306
Einzelheiten zu den Richtlinien 2306
Version der Richtlinie 2306
JSON-Richtliniendokument 2306
Weitere Informationen 2307
AWSMarketplacePurchaseOrdersServiceRolePolicy 2307
Diese Richtlinie wird verwendet 2307
Einzelheiten der Richtlinie 2307
Version der Richtlinie 2308
JSON-Richtliniendokument 2308
Weitere Informationen 2308
AWSMarketplaceRead-only 2309
Diese Richtlinie wird verwendet 2309
Einzelheiten zu den Richtlinien 2309
Version der Richtlinie 2309
JSON-Richtliniendokument 2309
Weitere Informationen 2310

AWSMarketplaceResaleAuthorizationServiceRolePolicy 2311
Diese Richtlinie wird verwendet 2311
Einzelheiten der Richtlinie 2311
Version der Richtlinie 2311
JSON-Richtliniendokument 2311
Weitere Informationen 2314
AWSMarketplaceSellerFullAccess 2314
Diese Richtlinie wird verwendet 2314
Einzelheiten zu den Richtlinien 2314
Version der Richtlinie 2314
JSON-Richtliniendokument 2315
Weitere Informationen 2318
AWSMarketplaceSellerProductsFullAccess 2318
Diese Richtlinie wird verwendet 2318
Einzelheiten zu den Richtlinien 2319
Version der Richtlinie 2319
JSON-Richtliniendokument 2319
Weitere Informationen 2321
AWSMarketplaceSellerProductsReadOnly 2321
Diese Richtlinie wird verwendet 2321
Einzelheiten zu den Richtlinien 2321
Version der Richtlinie 2322
JSON-Richtliniendokument 2322
Weitere Informationen 2322
AWSMediaConnectServicePolicy 2323
Diese Richtlinie wird verwendet 2323
Einzelheiten der Richtlinie 2323
Version der Richtlinie 2323
JSON-Richtliniendokument 2324
Weitere Informationen 2325
AWSMediaTailorServiceRolePolicy 2325
Diese Richtlinie wird verwendet 2325
Einzelheiten der Richtlinie 2325
Version der Richtlinie 2326
JSON-Richtliniendokument 2326
Weitere Informationen 2326

AWSMigrationHubDiscoveryAccess 2327
Diese Richtlinie wird verwendet 2327
Einzelheiten zu den Richtlinien 2327
Version der Richtlinie 2327
JSON-Richtliniendokument 2327
Weitere Informationen 2329
AWSMigrationHubDMSAccess 2329
Diese Richtlinie wird verwendet 2329
Einzelheiten zu den Richtlinien 2329
Version der Richtlinie 2329
JSON-Richtliniendokument 2330
Weitere Informationen 2331
AWSMigrationHubFullAccess 2331
Diese Richtlinie wird verwendet 2331
Einzelheiten zu den Richtlinien 2331
Version der Richtlinie 2331
JSON-Richtliniendokument 2332
Weitere Informationen 2333
AWSMigrationHubOrchestratorConsoleFullAccess 2333
Diese Richtlinie wird verwendet 2333
Einzelheiten zu den Richtlinien 2333
Version der Richtlinie 2334
JSON-Richtliniendokument 2334
Weitere Informationen 2337
AWSMigrationHubOrchestratorInstanceRolePolicy 2337
Diese Richtlinie wird verwendet 2337
Einzelheiten zu den Richtlinien 2337
Version der Richtlinie 2338
JSON-Richtliniendokument 2338
Weitere Informationen 2339
AWSMigrationHubOrchestratorPlugin 2339
Diese Richtlinie wird verwendet 2339
Einzelheiten zu den Richtlinien 2339
Version der Richtlinie 2339
JSON-Richtliniendokument 2340
Weitere Informationen 2341

AWSMigrationHubOrchestratorServiceRolePolicy 2341
Diese Richtlinie wird verwendet 2341
Einzelheiten der Richtlinie 2341
Version der Richtlinie 2342
JSON-Richtliniendokument 2342
Weitere Informationen 2345
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess 2345
Diese Richtlinie wird verwendet 2346
Einzelheiten zu den Richtlinien 2346
Version der Richtlinie 2346
JSON-Richtliniendokument 2346
Weitere Informationen 2352
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy 2352
Diese Richtlinie wird verwendet 2352
Einzelheiten zu den Richtlinien 2352
Version der Richtlinie 2353
JSON-Richtliniendokument 2353
Weitere Informationen 2354
AWSMigrationHubRefactorSpacesFullAccess 2355
Diese Richtlinie wird verwendet 2355
Einzelheiten zu den Richtlinien 2355
Version der Richtlinie 2355
JSON-Richtliniendokument 2355
Weitere Informationen 2362
AWSMigrationHubRefactorSpacesServiceRolePolicy 2362
Diese Richtlinie wird verwendet 2362
Einzelheiten der Richtlinie 2362
Version der Richtlinie 2363
JSON-Richtliniendokument 2363
Weitere Informationen 2366
AWSMigrationHubSMSAccess 2367
Diese Richtlinie wird verwendet 2367
Einzelheiten zu den Richtlinien 2367
Version der Richtlinie 2367
JSON-Richtliniendokument 2367
Weitere Informationen 2368

AWSMigrationHubStrategyCollector ... 2369
Diese Richtlinie wird verwendet ... 2369
Einzelheiten zu den Richtlinien ... 2369
Version der Richtlinie ... 2369
JSON-Richtliniendokument ... 2369
Weitere Informationen ... 2372
AWSMigrationHubStrategyConsoleFullAccess ... 2372
Diese Richtlinie wird verwendet ... 2372
Einzelheiten zu den Richtlinien ... 2372
Version der Richtlinie ... 2372
JSON-Richtliniendokument ... 2373
Weitere Informationen ... 2374
AWSMigrationHubStrategyServiceRolePolicy ... 2375
Diese Richtlinie wird verwendet ... 2375
Einzelheiten der Richtlinie ... 2375
Version der Richtlinie ... 2375
JSON-Richtliniendokument ... 2375
Weitere Informationen ... 2376
AWSMobileHub_FullAccess ... 2376
Diese Richtlinie wird verwendet ... 2377
Einzelheiten zu den Richtlinien ... 2377
Version der Richtlinie ... 2377
JSON-Richtliniendokument ... 2377
Weitere Informationen ... 2379
AWSMobileHub_ReadOnly ... 2379
Diese Richtlinie wird verwendet ... 2379
Einzelheiten zu den Richtlinien ... 2379
Version der Richtlinie ... 2379
JSON-Richtliniendokument ... 2380
Weitere Informationen ... 2381
AWSMSKReplicatorExecutionRole ... 2381
Diese Richtlinie wird verwendet ... 2381
Einzelheiten zu den Richtlinien ... 2381
Version der Richtlinie ... 2382
JSON-Richtliniendokument ... 2382
Weitere Informationen ... 2383

AWSNetworkFirewallServiceRolePolicy 2383
Diese Richtlinie wird verwendet 2384
Einzelheiten der Richtlinie 2384
Version der Richtlinie 2384
JSON-Richtliniendokument 2384
Weitere Informationen 2386
AWSNetworkManagerCloudWANServiceRolePolicy 2386
Diese Richtlinie wird verwendet 2386
Einzelheiten der Richtlinie 2386
Version der Richtlinie 2386
JSON-Richtliniendokument 2387
Weitere Informationen 2387
AWSNetworkManagerFullAccess 2387
Diese Richtlinie wird verwendet 2387
Einzelheiten zu den Richtlinien 2388
Version der Richtlinie 2388
JSON-Richtliniendokument 2388
Weitere Informationen 2389
AWSNetworkManagerReadOnlyAccess 2389
Diese Richtlinie wird verwendet 2389
Einzelheiten zu den Richtlinien 2389
Version der Richtlinie 2389
JSON-Richtliniendokument 2390
Weitere Informationen 2390
AWSNetworkManagerServiceRolePolicy 2390
Diese Richtlinie wird verwendet 2390
Einzelheiten der Richtlinie 2391
Version der Richtlinie 2391
JSON-Richtliniendokument 2391
Weitere Informationen 2392
AWSOpsWorks_FullAccess 2392
Diese Richtlinie wird verwendet 2392
Einzelheiten zu den Richtlinien 2392
Version der Richtlinie 2393
JSON-Richtliniendokument 2393
Weitere Informationen 2394

AWSOpsWorksCloudWatchLogs 2394
Diese Richtlinie wird verwendet 2394
Einzelheiten zu den Richtlinien 2394
Version der Richtlinie 2395
JSON-Richtliniendokument 2395
Weitere Informationen 2395
AWSOpsWorksCMInstanceProfileRole 2396
Diese Richtlinie wird verwendet 2396
Einzelheiten zu den Richtlinien 2396
Version der Richtlinie 2396
JSON-Richtliniendokument 2396
Weitere Informationen 2397
AWSOpsWorksCMServiceRole 2397
Diese Richtlinie wird verwendet 2398
Einzelheiten zu den Richtlinien 2398
Version der Richtlinie 2398
JSON-Richtliniendokument 2398
Weitere Informationen 2402
AWSOpsWorksInstanceRegistration 2403
Diese Richtlinie wird verwendet 2403
Einzelheiten zu den Richtlinien 2403
Version der Richtlinie 2403
JSON-Richtliniendokument 2403
Weitere Informationen 2404
AWSOpsWorksRegisterCLI_EC2 2404
Diese Richtlinie wird verwendet 2404
Einzelheiten zu den Richtlinien 2404
Version der Richtlinie 2404
JSON-Richtliniendokument 2405
Weitere Informationen 2405
AWSOpsWorksRegisterCLI_OnPremises 2406
Diese Richtlinie wird verwendet 2406
Einzelheiten zu den Richtlinien 2406
Version der Richtlinie 2406
JSON-Richtliniendokument 2406
Weitere Informationen 2408

AWSOrganizationsFullAccess 2408
Diese Richtlinie wird verwendet 2408
Einzelheiten zu den Richtlinien 2408
Version der Richtlinie 2409
JSON-Richtliniendokument 2409
Weitere Informationen 2410
AWSOrganizationsReadOnlyAccess 2410
Diese Richtlinie wird verwendet 2410
Einzelheiten zu den Richtlinien 2410
Version der Richtlinie 2411
JSON-Richtliniendokument 2411
Weitere Informationen 2411
AWSOrganizationsServiceTrustPolicy 2412
Diese Richtlinie wird verwendet 2412
Einzelheiten der Richtlinie 2412
Version der Richtlinie 2412
JSON-Richtliniendokument 2413
Weitere Informationen 2413
AWSOutpostsAuthorizeServerPolicy 2413
Diese Richtlinie wird verwendet 2414
Einzelheiten zu den Richtlinien 2414
Version der Richtlinie 2414
JSON-Richtliniendokument 2414
Weitere Informationen 2415
AWSOutpostsServiceRolePolicy 2415
Diese Richtlinie wird verwendet 2415
Einzelheiten der Richtlinie 2415
Version der Richtlinie 2415
JSON-Richtliniendokument 2416
Weitere Informationen 2416
AWSPanoramaApplianceRolePolicy 2416
Diese Richtlinie wird verwendet 2416
Einzelheiten zu den Richtlinien 2416
Version der Richtlinie 2417
JSON-Richtliniendokument 2417
Weitere Informationen 2417

AWSPanoramaApplianceServiceRolePolicy 2418
Diese Richtlinie wird verwendet 2418
Einzelheiten zu den Richtlinien 2418
Version der Richtlinie 2418
JSON-Richtliniendokument 2419
Weitere Informationen 2420
AWSPanoramaFullAccess 2420
Diese Richtlinie wird verwendet 2420
Einzelheiten zu den Richtlinien 2420
Version der Richtlinie 2421
JSON-Richtliniendokument 2421
Weitere Informationen 2423
AWSPanoramaGreengrassGroupRolePolicy 2424
Diese Richtlinie wird verwendet 2424
Einzelheiten zu den Richtlinien 2424
Version der Richtlinie 2424
JSON-Richtliniendokument 2424
Weitere Informationen 2426
AWSPanoramaSageMakerRolePolicy 2426
Diese Richtlinie wird verwendet 2426
Einzelheiten zu den Richtlinien 2426
Version der Richtlinie 2426
JSON-Richtliniendokument 2427
Weitere Informationen 2427
AWSPanoramaServiceLinkedRolePolicy 2427
Diese Richtlinie wird verwendet 2428
Einzelheiten der Richtlinie 2428
Version der Richtlinie 2428
JSON-Richtliniendokument 2428
Weitere Informationen 2431
AWSPanoramaServiceRolePolicy 2431
Diese Richtlinie wird verwendet 2431
Einzelheiten zu den Richtlinien 2431
Version der Richtlinie 2431
JSON-Richtliniendokument 2432
Weitere Informationen 2439

AWSPriceListServiceFullAccess 2439
Diese Richtlinie wird verwendet 2439
Einzelheiten zu den Richtlinien 2439
Version der Richtlinie 2439
JSON-Richtliniendokument 2440
Weitere Informationen 2440
AWSPrivateCAAuditor 2440
Diese Richtlinie wird verwendet 2440
Einzelheiten zu den Richtlinien 2440
Version der Richtlinie 2441
JSON-Richtliniendokument 2441
Weitere Informationen 2442
AWSPrivateCAFullAccess 2442
Diese Richtlinie wird verwendet 2442
Einzelheiten zu den Richtlinien 2442
Version der Richtlinie 2442
JSON-Richtliniendokument 2443
Weitere Informationen 2443
AWSPrivateCAPrivilegedUser 2443
Diese Richtlinie wird verwendet 2443
Einzelheiten zu den Richtlinien 2443
Version der Richtlinie 2444
JSON-Richtliniendokument 2444
Weitere Informationen 2445
AWSPrivateCAReadOnly 2445
Diese Richtlinie wird verwendet 2446
Einzelheiten zu den Richtlinien 2446
Version der Richtlinie 2446
JSON-Richtliniendokument 2446
Weitere Informationen 2447
AWSPrivateCAUser 2447
Diese Richtlinie wird verwendet 2447
Einzelheiten zu den Richtlinien 2447
Version der Richtlinie 2447
JSON-Richtliniendokument 2448
Weitere Informationen 2449

AWSPrivateMarketplaceAdminFullAccess 2449
Diese Richtlinie wird verwendet 2449
Einzelheiten zu den Richtlinien 2449
Version der Richtlinie 2450
JSON-Richtliniendokument 2450
Weitere Informationen 2451
AWSPrivateMarketplaceRequests 2451
Diese Richtlinie wird verwendet 2452
Einzelheiten zu den Richtlinien 2452
Version der Richtlinie 2452
JSON-Richtliniendokument 2452
Weitere Informationen 2453
AWSPrivateNetworksServiceRolePolicy 2453
Diese Richtlinie wird verwendet 2453
Einzelheiten der Richtlinie 2453
Version der Richtlinie 2453
JSON-Richtliniendokument 2454
Weitere Informationen 2454
AWSProtonCodeBuildProvisioningBasicAccess 2454
Diese Richtlinie wird verwendet 2454
Einzelheiten zu den Richtlinien 2455
Version der Richtlinie 2455
JSON-Richtliniendokument 2455
Weitere Informationen 2456
AWSProtonCodeBuildProvisioningServiceRolePolicy 2456
Diese Richtlinie wird verwendet 2456
Einzelheiten der Richtlinie 2456
Version der Richtlinie 2456
JSON-Richtliniendokument 2457
Weitere Informationen 2458
AWSProtonDeveloperAccess 2458
Diese Richtlinie wird verwendet 2458
Einzelheiten zu den Richtlinien 2458
Version der Richtlinie 2459
JSON-Richtliniendokument 2459
Weitere Informationen 2461

AWSProtonFullAccess 2461
Diese Richtlinie wird verwendet 2462
Einzelheiten zu den Richtlinien 2462
Version der Richtlinie 2462
JSON-Richtliniendokument 2462
Weitere Informationen 2464
AWSProtonReadOnlyAccess 2464
Diese Richtlinie wird verwendet 2465
Einzelheiten zu den Richtlinien 2465
Version der Richtlinie 2465
JSON-Richtliniendokument 2465
Weitere Informationen 2466
AWSProtonServiceGitSyncServiceRolePolicy 2467
Diese Richtlinie wird verwendet 2467
Einzelheiten der Richtlinie 2467
Version der Richtlinie 2467
JSON-Richtliniendokument 2468
Weitere Informationen 2468
AWSProtonSyncServiceRolePolicy 2468
Diese Richtlinie wird verwendet 2469
Einzelheiten der Richtlinie 2469
Version der Richtlinie 2469
JSON-Richtliniendokument 2469
Weitere Informationen 2470
AWSPurchaseOrdersServiceRolePolicy 2470
Diese Richtlinie wird verwendet 2471
Einzelheiten zu den Richtlinien 2471
Version der Richtlinie 2471
JSON-Richtliniendokument 2471
Weitere Informationen 2472
AWSQuickSightAssetBundleExportPolicy 2472
Diese Richtlinie wird verwendet 2472
Einzelheiten zu den Richtlinien 2472
Version der Richtlinie 2473
JSON-Richtliniendokument 2473
Weitere Informationen 2475

AWSQuickSightAssetBundleImportPolicy 2475
Diese Richtlinie wird verwendet 2475
Einzelheiten zu den Richtlinien 2476
Version der Richtlinie 2476
JSON-Richtliniendokument 2476
Weitere Informationen 2479
AWSQuicksightAthenaAccess 2479
Diese Richtlinie wird verwendet 2479
Einzelheiten zu den Richtlinien 2479
Version der Richtlinie 2480
JSON-Richtliniendokument 2480
Weitere Informationen 2482
AWSQuickSightDescribeRDS 2482
Diese Richtlinie wird verwendet 2482
Einzelheiten zu den Richtlinien 2482
Version der Richtlinie 2483
JSON-Richtliniendokument 2483
Weitere Informationen 2483
AWSQuickSightDescribeRedshift 2484
Diese Richtlinie wird verwendet 2484
Einzelheiten zu den Richtlinien 2484
Version der Richtlinie 2484
JSON-Richtliniendokument 2484
Weitere Informationen 2485
AWSQuickSightElasticsearchPolicy 2485
Diese Richtlinie wird verwendet 2485
Einzelheiten zu den Richtlinien 2485
Version der Richtlinie 2485
JSON-Richtliniendokument 2486
Weitere Informationen 2487
AWSQuickSightIoTAnalyticsAccess 2487
Diese Richtlinie wird verwendet 2487
Einzelheiten zu den Richtlinien 2487
Version der Richtlinie 2487
JSON-Richtliniendokument 2488
Weitere Informationen 2488

AWSQuickSightListIAM 2488
Diese Richtlinie wird verwendet 2489
Einzelheiten zu den Richtlinien 2489
Version der Richtlinie 2489
JSON-Richtliniendokument 2489
Weitere Informationen 2489
AWSQuicksightOpenSearchPolicy 2490
Diese Richtlinie wird verwendet 2490
Einzelheiten zu den Richtlinien 2490
Version der Richtlinie 2490
JSON-Richtliniendokument 2490
Weitere Informationen 2491
AWSQuickSightSageMakerPolicy 2492
Diese Richtlinie wird verwendet 2492
Einzelheiten zu den Richtlinien 2492
Version der Richtlinie 2492
JSON-Richtliniendokument 2492
Weitere Informationen 2494
AWSQuickSightTimestreamPolicy 2494
Diese Richtlinie wird verwendet 2494
Einzelheiten zu den Richtlinien 2494
Version der Richtlinie 2494
JSON-Richtliniendokument 2495
Weitere Informationen 2495
AWSReachabilityAnalyzerServiceRolePolicy 2495
Diese Richtlinie wird verwendet 2496
Einzelheiten der Richtlinie 2496
Version der Richtlinie 2496
JSON-Richtliniendokument 2496
Weitere Informationen 2498
AWSRefactoringToolkitFullAccess 2499
Diese Richtlinie wird verwendet 2499
Einzelheiten zu den Richtlinien 2499
Version der Richtlinie 2499
JSON-Richtliniendokument 2500
Weitere Informationen 2513

AWSRefactoringToolkitSidecarPolicy 2513
Diese Richtlinie wird verwendet 2514
Einzelheiten zu den Richtlinien 2514
Version der Richtlinie 2514
JSON-Richtliniendokument 2514
Weitere Informationen 2515
AWSrePostPrivateCloudWatchAccess 2515
Diese Richtlinie wird verwendet 2515
Einzelheiten der Richtlinie 2516
Version der Richtlinie 2516
JSON-Richtliniendokument 2516
Weitere Informationen 2517
AWSRepostSpaceSupportOperationsPolicy 2517
Diese Richtlinie wird verwendet 2517
Einzelheiten zu den Richtlinien 2517
Version der Richtlinie 2517
JSON-Richtliniendokument 2518
Weitere Informationen 2518
AWSResilienceHubAsssessmentExecutionPolicy 2518
Diese Richtlinie wird verwendet 2519
Einzelheiten zu den Richtlinien 2519
Version der Richtlinie 2519
JSON-Richtliniendokument 2519
Weitere Informationen 2523
AWSResourceAccessManagerFullAccess 2523
Diese Richtlinie wird verwendet 2524
Einzelheiten zu den Richtlinien 2524
Version der Richtlinie 2524
JSON-Richtliniendokument 2524
Weitere Informationen 2524
AWSResourceAccessManagerReadOnlyAccess 2525
Diese Richtlinie wird verwendet 2525
Einzelheiten zu den Richtlinien 2525
Version der Richtlinie 2525
JSON-Richtliniendokument 2525
Weitere Informationen 2526

AWSResourceAccessManagerResourceShareParticipantAccess 2526
Diese Richtlinie wird verwendet 2526
Einzelheiten zu den Richtlinien 2526
Version der Richtlinie 2527
JSON-Richtliniendokument 2527
Weitere Informationen 2527
AWSResourceAccessManagerServiceRolePolicy 2528
Diese Richtlinie wird verwendet 2528
Einzelheiten der Richtlinie 2528
Version der Richtlinie 2528
JSON-Richtliniendokument 2528
Weitere Informationen 2529
AWSResourceExplorerFullAccess 2529
Diese Richtlinie wird verwendet 2530
Einzelheiten zu den Richtlinien 2530
Version der Richtlinie 2530
JSON-Richtliniendokument 2530
Weitere Informationen 2531
AWSResourceExplorerOrganizationsAccess 2531
Diese Richtlinie wird verwendet 2531
Einzelheiten zu den Richtlinien 2532
Version der Richtlinie 2532
JSON-Richtliniendokument 2532
Weitere Informationen 2534
AWSResourceExplorerReadOnlyAccess 2534
Diese Richtlinie wird verwendet 2534
Einzelheiten zu den Richtlinien 2534
Version der Richtlinie 2534
JSON-Richtliniendokument 2535
Weitere Informationen 2535
AWSResourceExplorerServiceRolePolicy 2535
Diese Richtlinie wird verwendet 2536
Einzelheiten der Richtlinie 2536
Version der Richtlinie 2536
JSON-Richtliniendokument 2536
Weitere Informationen 2545

AWSResourceGroupsReadOnlyAccess 2545
Diese Richtlinie wird verwendet 2546
Einzelheiten zu den Richtlinien 2546
Version der Richtlinie 2546
JSON-Richtliniendokument 2546
Weitere Informationen 2547
AWSRoboMaker_FullAccess 2548
Diese Richtlinie wird verwendet 2548
Einzelheiten zu den Richtlinien 2548
Version der Richtlinie 2548
JSON-Richtliniendokument 2548
Weitere Informationen 2550
AWSRoboMakerReadOnlyAccess 2550
Diese Richtlinie wird verwendet 2550
Einzelheiten zu den Richtlinien 2550
Version der Richtlinie 2550
JSON-Richtliniendokument 2551
Weitere Informationen 2551
AWSRoboMakerServicePolicy 2551
Diese Richtlinie wird verwendet 2552
Einzelheiten der Richtlinie 2552
Version der Richtlinie 2552
JSON-Richtliniendokument 2552
Weitere Informationen 2554
AWSRoboMakerServiceRolePolicy 2554
Diese Richtlinie wird verwendet 2554
Einzelheiten zu den Richtlinien 2554
Version der Richtlinie 2554
JSON-Richtliniendokument 2555
Weitere Informationen 2556
AWSRolesAnywhereServicePolicy 2556
Diese Richtlinie wird verwendet 2556
Einzelheiten der Richtlinie 2556
Version der Richtlinie 2557
JSON-Richtliniendokument 2557
Weitere Informationen 2558

AWSS3OnOutpostsServiceRolePolicy 2558
Diese Richtlinie wird verwendet 2558
Einzelheiten der Richtlinie 2558
Version der Richtlinie 2558
JSON-Richtliniendokument 2559
Weitere Informationen 2561
AWSSavingsPlansFullAccess 2561
Diese Richtlinie wird verwendet 2561
Einzelheiten zu den Richtlinien 2562
Version der Richtlinie 2562
JSON-Richtliniendokument 2562
Weitere Informationen 2562
AWSSavingsPlansReadOnlyAccess 2563
Diese Richtlinie wird verwendet 2563
Einzelheiten zu den Richtlinien 2563
Version der Richtlinie 2563
JSON-Richtliniendokument 2563
Weitere Informationen 2564
AWSSecurityHubFullAccess 2564
Diese Richtlinie wird verwendet 2564
Einzelheiten zu den Richtlinien 2564
Version der Richtlinie 2564
JSON-Richtliniendokument 2565
Weitere Informationen 2565
AWSSecurityHubOrganizationsAccess 2566
Diese Richtlinie wird verwendet 2566
Einzelheiten zu den Richtlinien 2566
Version der Richtlinie 2566
JSON-Richtliniendokument 2566
Weitere Informationen 2568
AWSSecurityHubReadOnlyAccess 2568
Diese Richtlinie wird verwendet 2568
Einzelheiten zu den Richtlinien 2568
Version der Richtlinie 2568
JSON-Richtliniendokument 2569
Weitere Informationen 2569

AWSSecurityHubServiceRolePolicy 2569
Diese Richtlinie wird verwendet 2569
Einzelheiten der Richtlinie 2570
Version der Richtlinie 2570
JSON-Richtliniendokument 2570
Weitere Informationen 2572
AWSServiceCatalogAdminFullAccess 2572
Diese Richtlinie wird verwendet 2572
Einzelheiten zu den Richtlinien 2572
Version der Richtlinie 2573
JSON-Richtliniendokument 2573
Weitere Informationen 2576
AWSServiceCatalogAdminReadOnlyAccess 2576
Diese Richtlinie wird verwendet 2576
Einzelheiten zu den Richtlinien 2576
Version der Richtlinie 2576
JSON-Richtliniendokument 2577
Weitere Informationen 2578
AWSServiceCatalogAppRegistryFullAccess 2578
Diese Richtlinie wird verwendet 2578
Einzelheiten zu den Richtlinien 2578
Version der Richtlinie 2579
JSON-Richtliniendokument 2579
Weitere Informationen 2581
AWSServiceCatalogAppRegistryReadOnlyAccess 2581
Diese Richtlinie wird verwendet 2581
Einzelheiten zu den Richtlinien 2581
Version der Richtlinie 2582
JSON-Richtliniendokument 2582
Weitere Informationen 2582
AWSServiceCatalogAppRegistryServiceRolePolicy 2583
Diese Richtlinie wird verwendet 2583
Einzelheiten der Richtlinie 2583
Version der Richtlinie 2583
JSON-Richtliniendokument 2583
Weitere Informationen 2585

AWSServiceCatalogEndUserFullAccess 2585
Diese Richtlinie wird verwendet 2585
Einzelheiten zu den Richtlinien 2585
Version der Richtlinie 2585
JSON-Richtliniendokument 2586
Weitere Informationen 2588
AWSServiceCatalogEndUserReadOnlyAccess 2588
Diese Richtlinie wird verwendet 2588
Einzelheiten zu den Richtlinien 2588
Version der Richtlinie 2588
JSON-Richtliniendokument 2589
Weitere Informationen 2590
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 2590
Diese Richtlinie wird verwendet 2591
Einzelheiten der Richtlinie 2591
Version der Richtlinie 2591
JSON-Richtliniendokument 2591
Weitere Informationen 2592
AWSServiceCatalogSyncServiceRolePolicy 2592
Diese Richtlinie wird verwendet 2592
Einzelheiten der Richtlinie 2592
Version der Richtlinie 2592
JSON-Richtliniendokument 2593
Weitere Informationen 2594
AWSServiceRoleForAmazonEKSNodegroup 2594
Diese Richtlinie wird verwendet 2594
Einzelheiten der Richtlinie 2594
Version der Richtlinie 2594
JSON-Richtliniendokument 2595
Weitere Informationen 2599
AWSServiceRoleForAmazonQDeveloper 2599
Diese Richtlinie wird verwendet 2599
Einzelheiten der Richtlinie 2599
Version der Richtlinie 2599
JSON-Richtliniendokument 2600
Weitere Informationen 2600

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy 2600
Diese Richtlinie wird verwendet 2601
Einzelheiten der Richtlinie 2601
Version der Richtlinie 2601
JSON-Richtliniendokument 2601
Weitere Informationen 2602
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy 2602
Diese Richtlinie wird verwendet 2602
Einzelheiten der Richtlinie 2602
Version der Richtlinie 2602
JSON-Richtliniendokument 2603
Weitere Informationen 2603
AWSServiceRoleForCodeGuru-Profiler 2603
Diese Richtlinie wird verwendet 2603
Einzelheiten der Richtlinie 2604
Version der Richtlinie 2604
JSON-Richtliniendokument 2604
Weitere Informationen 2604
AWSServiceRoleForCodeWhispererPolicy 2605
Diese Richtlinie wird verwendet 2605
Einzelheiten der Richtlinie 2605
Version der Richtlinie 2605
JSON-Richtliniendokument 2605
Weitere Informationen 2607
AWSServiceRoleForEC2ScheduledInstances 2607
Diese Richtlinie wird verwendet 2607
Einzelheiten der Richtlinie 2608
Version der Richtlinie 2608
JSON-Richtliniendokument 2608
Weitere Informationen 2609
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 2609
Diese Richtlinie wird verwendet 2609
Einzelheiten der Richtlinie 2609
Version der Richtlinie 2610
JSON-Richtliniendokument 2610
Weitere Informationen 2610

AWSServiceRoleForImageBuilder 2610
Diese Richtlinie wird verwendet 2611
Einzelheiten der Richtlinie 2611
Version der Richtlinie 2611
JSON-Richtliniendokument 2611
Weitere Informationen 2621
AWSServiceRoleForIoTSiteWise 2621
Diese Richtlinie wird verwendet 2621
Einzelheiten der Richtlinie 2621
Version der Richtlinie 2622
JSON-Richtliniendokument 2622
Weitere Informationen 2623
AWSServiceRoleForLogDeliveryPolicy 2623
Diese Richtlinie wird verwendet 2623
Einzelheiten der Richtlinie 2624
Version der Richtlinie 2624
JSON-Richtliniendokument 2624
Weitere Informationen 2625
AWSServiceRoleForMonitronPolicy 2625
Diese Richtlinie wird verwendet 2625
Einzelheiten der Richtlinie 2625
Version der Richtlinie 2625
JSON-Richtliniendokument 2626
Weitere Informationen 2626
AWSServiceRoleForNeptuneGraphPolicy 2626
Diese Richtlinie wird verwendet 2626
Einzelheiten der Richtlinie 2627
Version der Richtlinie 2627
JSON-Richtliniendokument 2627
Weitere Informationen 2628
AWSServiceRoleForPrivateMarketplaceAdminPolicy 2629
Diese Richtlinie wird verwendet 2629
Einzelheiten der Richtlinie 2629
Version der Richtlinie 2629
JSON-Richtliniendokument 2629
Weitere Informationen 2631

AWSServiceRoleForSMS 2631
Diese Richtlinie wird verwendet 2631
Einzelheiten der Richtlinie 2631
Version der Richtlinie 2632
JSON-Richtliniendokument 2632
Weitere Informationen 2639
AWSServiceRoleForUserSubscriptions 2639
Diese Richtlinie wird verwendet 2639
Einzelheiten der Richtlinie 2639
Version der Richtlinie 2639
JSON-Richtliniendokument 2640
Weitere Informationen 2640
AWSServiceRolePolicyForBackupReports 2640
Diese Richtlinie wird verwendet 2641
Einzelheiten der Richtlinie 2641
Version der Richtlinie 2641
JSON-Richtliniendokument 2641
Weitere Informationen 2642
AWSServiceRolePolicyForBackupRestoreTesting 2643
Diese Richtlinie wird verwendet 2643
Einzelheiten der Richtlinie 2643
Version der Richtlinie 2643
JSON-Richtliniendokument 2643
Weitere Informationen 2646
AWSShieldDRTAccessPolicy 2646
Diese Richtlinie wird verwendet 2646
Einzelheiten zu den Richtlinien 2647
Version der Richtlinie 2647
JSON-Richtliniendokument 2647
Weitere Informationen 2648
AWSShieldServiceRolePolicy 2648
Diese Richtlinie wird verwendet 2648
Einzelheiten der Richtlinie 2648
Version der Richtlinie 2649
JSON-Richtliniendokument 2649
Weitere Informationen 2649

AWSSSMForSAPServiceLinkedRolePolicy 2650
Diese Richtlinie wird verwendet 2650
Einzelheiten der Richtlinie 2650
Version der Richtlinie 2650
JSON-Richtliniendokument 2650
Weitere Informationen 2657
AWSSSMOpsInsightsServiceRolePolicy 2657
Diese Richtlinie wird verwendet 2657
Einzelheiten der Richtlinie 2657
Version der Richtlinie 2657
JSON-Richtliniendokument 2658
Weitere Informationen 2658
AWSSSODirectoryAdministrator 2659
Diese Richtlinie wird verwendet 2659
Einzelheiten zu den Richtlinien 2659
Version der Richtlinie 2659
JSON-Richtliniendokument 2659
Weitere Informationen 2660
AWSSSODirectoryReadOnly 2660
Diese Richtlinie wird verwendet 2660
Einzelheiten zu den Richtlinien 2660
Version der Richtlinie 2660
JSON-Richtliniendokument 2661
Weitere Informationen 2661
AWSSSOMasterAccountAdministrator 2661
Diese Richtlinie wird verwendet 2662
Einzelheiten zu den Richtlinien 2662
Version der Richtlinie 2662
JSON-Richtliniendokument 2662
Weitere Informationen 2664
AWSSSOMemberAccountAdministrator 2664
Diese Richtlinie wird verwendet 2664
Einzelheiten zu den Richtlinien 2664
Version der Richtlinie 2665
JSON-Richtliniendokument 2665
Weitere Informationen 2666

AWSSSOReadOnly 2666
Diese Richtlinie wird verwendet 2666
Einzelheiten zu den Richtlinien 2667
Version der Richtlinie 2667
JSON-Richtliniendokument 2667
Weitere Informationen 2668
AWSSSOServiceRolePolicy 2668
Diese Richtlinie wird verwendet 2668
Einzelheiten der Richtlinie 2668
Version der Richtlinie 2669
JSON-Richtliniendokument 2669
Weitere Informationen 2672
AWSStepFunctionsConsoleFullAccess 2672
Diese Richtlinie wird verwendet 2673
Einzelheiten zu den Richtlinien 2673
Version der Richtlinie 2673
JSON-Richtliniendokument 2673
Weitere Informationen 2674
AWSStepFunctionsFullAccess 2674
Diese Richtlinie wird verwendet 2674
Einzelheiten zu den Richtlinien 2674
Version der Richtlinie 2675
JSON-Richtliniendokument 2675
Weitere Informationen 2675
AWSStepFunctionsReadOnlyAccess 2675
Diese Richtlinie wird verwendet 2676
Einzelheiten zu den Richtlinien 2676
Version der Richtlinie 2676
JSON-Richtliniendokument 2676
Weitere Informationen 2677
AWSStorageGatewayFullAccess 2677
Diese Richtlinie wird verwendet 2677
Einzelheiten zu den Richtlinien 2677
Version der Richtlinie 2678
JSON-Richtliniendokument 2678
Weitere Informationen 2678

AWSStorageGatewayReadOnlyAccess 2679
Diese Richtlinie wird verwendet 2679
Einzelheiten zu den Richtlinien 2679
Version der Richtlinie 2679
JSON-Richtliniendokument 2679
Weitere Informationen 2680
AWSStorageGatewayServiceRolePolicy 2680
Diese Richtlinie wird verwendet 2681
Einzelheiten der Richtlinie 2681
Version der Richtlinie 2681
JSON-Richtliniendokument 2681
Weitere Informationen 2682
AWSSupplyChainFederationAdminAccess 2682
Diese Richtlinie wird verwendet 2682
Einzelheiten zu den Richtlinien 2682
Version der Richtlinie 2682
JSON-Richtliniendokument 2683
Weitere Informationen 2688
AWSSupportAccess 2688
Diese Richtlinie wird verwendet 2688
Einzelheiten zu den Richtlinien 2688
Version der Richtlinie 2689
JSON-Richtliniendokument 2689
Weitere Informationen 2689
AWSSupportAppFullAccess 2689
Diese Richtlinie wird verwendet 2690
Einzelheiten zu den Richtlinien 2690
Version der Richtlinie 2690
JSON-Richtliniendokument 2690
Weitere Informationen 2691
AWSSupportAppReadOnlyAccess 2691
Diese Richtlinie wird verwendet 2691
Einzelheiten zu den Richtlinien 2691
Version der Richtlinie 2692
JSON-Richtliniendokument 2692
Weitere Informationen 2692

AWSSupportPlansFullAccess 2693
Diese Richtlinie wird verwendet 2693
Einzelheiten zu den Richtlinien 2693
Version der Richtlinie 2693
JSON-Richtliniendokument 2693
Weitere Informationen 2694
AWSSupportPlansReadOnlyAccess 2694
Diese Richtlinie wird verwendet 2694
Einzelheiten zu den Richtlinien 2694
Version der Richtlinie 2694
JSON-Richtliniendokument 2695
Weitere Informationen 2695
AWSSupportServiceRolePolicy 2695
Diese Richtlinie wird verwendet 2695
Einzelheiten der Richtlinie 2696
Version der Richtlinie 2696
JSON-Richtliniendokument 2696
Weitere Informationen 2771
AWSSystemsManagerAccountDiscoveryServicePolicy 2771
Diese Richtlinie wird verwendet 2772
Einzelheiten der Richtlinie 2772
Version der Richtlinie 2772
JSON-Richtliniendokument 2772
Weitere Informationen 2773
AWSSystemsManagerChangeManagementServicePolicy 2773
Diese Richtlinie wird verwendet 2773
Einzelheiten der Richtlinie 2773
Version der Richtlinie 2774
JSON-Richtliniendokument 2774
Weitere Informationen 2775
AWSSystemsManagerForSAPFullAccess 2776
Diese Richtlinie wird verwendet 2776
Einzelheiten zu den Richtlinien 2776
Version der Richtlinie 2776
JSON-Richtliniendokument 2776
Weitere Informationen 2777

AWSSystemsManagerForSAPReadOnlyAccess 2777
Diese Richtlinie wird verwendet 2777
Einzelheiten zu den Richtlinien 2777
Version der Richtlinie 2778
JSON-Richtliniendokument 2778
Weitere Informationen 2778
AWSSystemsManagerOpsDataSyncServiceRolePolicy 2779
Diese Richtlinie wird verwendet 2779
Einzelheiten der Richtlinie 2779
Version der Richtlinie 2779
JSON-Richtliniendokument 2779
Weitere Informationen 2783
AWSThinkboxAssetServerPolicy 2783
Diese Richtlinie wird verwendet 2783
Einzelheiten zu den Richtlinien 2783
Version der Richtlinie 2784
JSON-Richtliniendokument 2784
Weitere Informationen 2784
AWSThinkboxAWSPortalAdminPolicy 2785
Diese Richtlinie wird verwendet 2785
Einzelheiten zu den Richtlinien 2785
Version der Richtlinie 2785
JSON-Richtliniendokument 2785
Weitere Informationen 2795
AWSThinkboxAWSPortalGatewayPolicy 2796
Diese Richtlinie wird verwendet 2796
Einzelheiten zu den Richtlinien 2796
Version der Richtlinie 2796
JSON-Richtliniendokument 2796
Weitere Informationen 2798
AWSThinkboxAWSPortalWorkerPolicy 2798
Diese Richtlinie wird verwendet 2798
Einzelheiten zu den Richtlinien 2799
Version der Richtlinie 2799
JSON-Richtliniendokument 2799
Weitere Informationen 2801

AWSThinkboxDeadlineResourceTrackerAccessPolicy 2801
Diese Richtlinie wird verwendet 2801
Einzelheiten zu den Richtlinien 2801
Version der Richtlinie 2802
JSON-Richtliniendokument 2802
Weitere Informationen 2805
AWSThinkboxDeadlineResourceTrackerAdminPolicy 2805
Diese Richtlinie wird verwendet 2805
Einzelheiten zu den Richtlinien 2805
Version der Richtlinie 2805
JSON-Richtliniendokument 2806
Weitere Informationen 2811
AWSThinkboxDeadlineSpotEventPluginAdminPolicy 2812
Diese Richtlinie wird verwendet 2812
Einzelheiten zu den Richtlinien 2812
Version der Richtlinie 2812
JSON-Richtliniendokument 2812
Weitere Informationen 2815
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 2815
Diese Richtlinie wird verwendet 2816
Einzelheiten zu den Richtlinien 2816
Version der Richtlinie 2816
JSON-Richtliniendokument 2816
Weitere Informationen 2817
AWSTransferConsoleFullAccess 2818
Diese Richtlinie wird verwendet 2818
Einzelheiten zu den Richtlinien 2818
Version der Richtlinie 2818
JSON-Richtliniendokument 2818
Weitere Informationen 2819
AWSTransferFullAccess 2820
Diese Richtlinie wird verwendet 2820
Einzelheiten zu den Richtlinien 2820
Version der Richtlinie 2820
JSON-Richtliniendokument 2820
Weitere Informationen 2821

AWSTransferLoggingAccess 2821
Diese Richtlinie wird verwendet 2821
Einzelheiten zu den Richtlinien 2822
Version der Richtlinie 2822
JSON-Richtliniendokument 2822
Weitere Informationen 2822
AWSTransferReadOnlyAccess 2823
Diese Richtlinie wird verwendet 2823
Einzelheiten zu den Richtlinien 2823
Version der Richtlinie 2823
JSON-Richtliniendokument 2823
Weitere Informationen 2824
AWSTrustedAdvisorPriorityFullAccess 2824
Diese Richtlinie wird verwendet 2824
Einzelheiten zu den Richtlinien 2824
Version der Richtlinie 2825
JSON-Richtliniendokument 2825
Weitere Informationen 2827
AWSTrustedAdvisorPriorityReadOnlyAccess 2827
Diese Richtlinie wird verwendet 2827
Einzelheiten zu den Richtlinien 2827
Version der Richtlinie 2827
JSON-Richtliniendokument 2828
Weitere Informationen 2829
AWSTrustedAdvisorReportingServiceRolePolicy 2829
Diese Richtlinie wird verwendet 2829
Einzelheiten der Richtlinie 2829
Version der Richtlinie 2829
JSON-Richtliniendokument 2830
Weitere Informationen 2830
AWSTrustedAdvisorServiceRolePolicy 2830
Diese Richtlinie wird verwendet 2831
Einzelheiten der Richtlinie 2831
Version der Richtlinie 2831
JSON-Richtliniendokument 2831
Weitere Informationen 2834

AWSUserNotificationsServiceLinkedRolePolicy 2834
Diese Richtlinie wird verwendet 2834
Einzelheiten der Richtlinie 2835
Version der Richtlinie 2835
JSON-Richtliniendokument 2835
Weitere Informationen 2836
AWSVendorInsightsAssessorFullAccess 2836
Diese Richtlinie wird verwendet 2836
Einzelheiten zu den Richtlinien 2836
Version der Richtlinie 2836
JSON-Richtliniendokument 2837
Weitere Informationen 2838
AWSVendorInsightsAssessorReadOnly 2838
Diese Richtlinie wird verwendet 2838
Einzelheiten zu den Richtlinien 2838
Version der Richtlinie 2838
JSON-Richtliniendokument 2839
Weitere Informationen 2839
AWSVendorInsightsVendorFullAccess 2840
Diese Richtlinie wird verwendet 2840
Einzelheiten zu den Richtlinien 2840
Version der Richtlinie 2840
JSON-Richtliniendokument 2840
Weitere Informationen 2842
AWSVendorInsightsVendorReadOnly 2842
Diese Richtlinie wird verwendet 2842
Einzelheiten zu den Richtlinien 2842
Version der Richtlinie 2843
JSON-Richtliniendokument 2843
Weitere Informationen 2844
AWSVpcLatticeServiceRolePolicy 2844
Diese Richtlinie wird verwendet 2844
Einzelheiten der Richtlinie 2844
Version der Richtlinie 2845
JSON-Richtliniendokument 2845
Weitere Informationen 2845

AWSVPCS2SVpnServiceRolePolicy 2845
Diese Richtlinie wird verwendet 2846
Einzelheiten der Richtlinie 2846
Version der Richtlinie 2846
JSON-Richtliniendokument 2846
Weitere Informationen 2847
AWSVPCTransitGatewayServiceRolePolicy 2847
Diese Richtlinie wird verwendet 2847
Einzelheiten der Richtlinie 2847
Version der Richtlinie 2847
JSON-Richtliniendokument 2848
Weitere Informationen 2848
AWSVPCVerifiedAccessServiceRolePolicy 2848
Diese Richtlinie wird verwendet 2849
Einzelheiten der Richtlinie 2849
Version der Richtlinie 2849
JSON-Richtliniendokument 2849
Weitere Informationen 2851
AWSWAFConsoleFullAccess 2851
Diese Richtlinie wird verwendet 2851
Einzelheiten zu den Richtlinien 2851
Version der Richtlinie 2852
JSON-Richtliniendokument 2852
Weitere Informationen 2854
AWSWAFConsoleReadOnlyAccess 2854
Diese Richtlinie wird verwendet 2854
Einzelheiten zu den Richtlinien 2854
Version der Richtlinie 2855
JSON-Richtliniendokument 2855
Weitere Informationen 2856
AWSWAFFullAccess 2856
Diese Richtlinie wird verwendet 2856
Einzelheiten zu den Richtlinien 2856
Version der Richtlinie 2856
JSON-Richtliniendokument 2857
Weitere Informationen 2858

AWSWAFReadOnlyAccess 2859
Diese Richtlinie wird verwendet 2859
Einzelheiten zu den Richtlinien 2859
Version der Richtlinie 2859
JSON-Richtliniendokument 2859
Weitere Informationen 2860
AWSWellArchitectedDiscoveryServiceRolePolicy 2860
Diese Richtlinie wird verwendet 2860
Einzelheiten der Richtlinie 2861
Version der Richtlinie 2861
JSON-Richtliniendokument 2861
Weitere Informationen 2862
AWSWellArchitectedOrganizationsServiceRolePolicy 2863
Diese Richtlinie wird verwendet 2863
Einzelheiten der Richtlinie 2863
Version der Richtlinie 2863
JSON-Richtliniendokument 2863
Weitere Informationen 2864
AWSWickrFullAccess 2864
Diese Richtlinie wird verwendet 2864
Einzelheiten zu den Richtlinien 2864
Version der Richtlinie 2865
JSON-Richtliniendokument 2865
Weitere Informationen 2865
AWSXrayCrossAccountSharingConfiguration 2865
Diese Richtlinie wird verwendet 2866
Einzelheiten zu den Richtlinien 2866
Version der Richtlinie 2866
JSON-Richtliniendokument 2866
Weitere Informationen 2867
AWSXRayDaemonWriteAccess 2867
Diese Richtlinie wird verwendet 2867
Einzelheiten zu den Richtlinien 2868
Version der Richtlinie 2868
JSON-Richtliniendokument 2868
Weitere Informationen 2869

AWSXrayFullAccess 2869
Diese Richtlinie wird verwendet 2869
Einzelheiten zu den Richtlinien 2869
Version der Richtlinie 2869
JSON-Richtliniendokument 2870
Weitere Informationen 2870
AWSXrayReadOnlyAccess 2870
Diese Richtlinie wird verwendet 2870
Einzelheiten zu den Richtlinien 2871
Version der Richtlinie 2871
JSON-Richtliniendokument 2871
Weitere Informationen 2872
AWSXrayWriteOnlyAccess 2872
Diese Richtlinie wird verwendet 2872
Einzelheiten zu den Richtlinien 2872
Version der Richtlinie 2873
JSON-Richtliniendokument 2873
Weitere Informationen 2873
AWSZonalAutoshiftPracticeRunSLRPolicy 2874
Diese Richtlinie wird verwendet 2874
Einzelheiten der Richtlinie 2874
Version der Richtlinie 2874
JSON-Richtliniendokument 2874
Weitere Informationen 2875
BatchServiceRolePolicy 2875
Diese Richtlinie wird verwendet 2875
Einzelheiten der Richtlinie 2876
Version der Richtlinie 2876
JSON-Richtliniendokument 2876
Weitere Informationen 2882
Billing 2882
Diese Richtlinie wird verwendet 2882
Einzelheiten zu den Richtlinien 2882
Version der Richtlinie 2883
JSON-Richtliniendokument 2883
Weitere Informationen 2886

CertificateManagerServiceRolePolicy 2886
Diese Richtlinie wird verwendet 2886
Einzelheiten der Richtlinie 2886
Version der Richtlinie 2886
JSON-Richtliniendokument 2887
Weitere Informationen 2887
ClientVPNServiceConnectionsRolePolicy 2887
Diese Richtlinie wird verwendet 2887
Einzelheiten der Richtlinie 2888
Version der Richtlinie 2888
JSON-Richtliniendokument 2888
Weitere Informationen 2888
ClientVPNServiceRolePolicy 2889
Diese Richtlinie wird verwendet 2889
Einzelheiten der Richtlinie 2889
Version der Richtlinie 2889
JSON-Richtliniendokument 2889
Weitere Informationen 2890
CloudFormationStackSetsOrgAdminServiceRolePolicy 2890
Diese Richtlinie wird verwendet 2891
Einzelheiten der Richtlinie 2891
Version der Richtlinie 2891
JSON-Richtliniendokument 2891
Weitere Informationen 2892
CloudFormationStackSetsOrgMemberServiceRolePolicy 2892
Diese Richtlinie wird verwendet 2892
Einzelheiten der Richtlinie 2892
Version der Richtlinie 2892
JSON-Richtliniendokument 2893
Weitere Informationen 2893
CloudFrontFullAccess 2894
Diese Richtlinie wird verwendet 2894
Einzelheiten zu den Richtlinien 2894
Version der Richtlinie 2894
JSON-Richtliniendokument 2894
Weitere Informationen 2895

CloudFrontReadOnlyAccess 2896
Diese Richtlinie wird verwendet 2896
Einzelheiten zu den Richtlinien 2896
Version der Richtlinie 2896
JSON-Richtliniendokument 2896
Weitere Informationen 2897
CloudHSMServiceRolePolicy 2897
Diese Richtlinie wird verwendet 2898
Einzelheiten der Richtlinie 2898
Version der Richtlinie 2898
JSON-Richtliniendokument 2898
Weitere Informationen 2899
CloudSearchFullAccess 2899
Diese Richtlinie wird verwendet 2899
Einzelheiten zu den Richtlinien 2899
Version der Richtlinie 2899
JSON-Richtliniendokument 2899
Weitere Informationen 2900
CloudSearchReadOnlyAccess 2900
Diese Richtlinie wird verwendet 2900
Einzelheiten zu den Richtlinien 2900
Version der Richtlinie 2901
JSON-Richtliniendokument 2901
Weitere Informationen 2901
CloudTrailServiceRolePolicy 2901
Diese Richtlinie wird verwendet 2902
Einzelheiten der Richtlinie 2902
Version der Richtlinie 2902
JSON-Richtliniendokument 2902
Weitere Informationen 2904
CloudWatch-CrossAccountAccess 2904
Diese Richtlinie wird verwendet 2904
Einzelheiten der Richtlinie 2904
Version der Richtlinie 2904
JSON-Richtliniendokument 2905
Weitere Informationen 2905

CloudWatchActionsEC2Access 2905
Diese Richtlinie wird verwendet 2905
Einzelheiten zu den Richtlinien 2906
Version der Richtlinie 2906
JSON-Richtliniendokument 2906
Weitere Informationen 2906
CloudWatchAgentAdminPolicy 2907
Diese Richtlinie wird verwendet 2907
Einzelheiten zu den Richtlinien 2907
Version der Richtlinie 2907
JSON-Richtliniendokument 2907
Weitere Informationen 2908
CloudWatchAgentServerPolicy 2909
Diese Richtlinie wird verwendet 2909
Einzelheiten zu den Richtlinien 2909
Version der Richtlinie 2909
JSON-Richtliniendokument 2909
Weitere Informationen 2910
CloudWatchApplicationInsightsFullAccess 2910
Diese Richtlinie wird verwendet 2911
Einzelheiten zu den Richtlinien 2911
Version der Richtlinie 2911
JSON-Richtliniendokument 2911
Weitere Informationen 2912
CloudWatchApplicationInsightsReadOnlyAccess 2913
Diese Richtlinie wird verwendet 2913
Einzelheiten zu den Richtlinien 2913
Version der Richtlinie 2913
JSON-Richtliniendokument 2913
Weitere Informationen 2914
CloudwatchApplicationInsightsServiceLinkedRolePolicy 2914
Diese Richtlinie wird verwendet 2914
Einzelheiten der Richtlinie 2914
Version der Richtlinie 2915
JSON-Richtliniendokument 2915
Weitere Informationen 2924

CloudWatchApplicationSignalsFullAccess 2925
Diese Richtlinie wird verwendet 2925
Einzelheiten zu den Richtlinien 2925
Version der Richtlinie 2925
JSON-Richtliniendokument 2925
Weitere Informationen 2928
CloudWatchApplicationSignalsReadOnlyAccess 2928
Diese Richtlinie wird verwendet 2929
Einzelheiten zu den Richtlinien 2929
Version der Richtlinie 2929
JSON-Richtliniendokument 2929
Weitere Informationen 2931
CloudWatchApplicationSignalsServiceRolePolicy 2932
Diese Richtlinie wird verwendet 2932
Einzelheiten der Richtlinie 2932
Version der Richtlinie 2932
JSON-Richtliniendokument 2932
Weitere Informationen 2935
CloudWatchAutomaticDashboardsAccess 2935
Diese Richtlinie wird verwendet 2935
Einzelheiten zu den Richtlinien 2935
Version der Richtlinie 2935
JSON-Richtliniendokument 2936
Weitere Informationen 2937
CloudWatchCrossAccountSharingConfiguration 2937
Diese Richtlinie wird verwendet 2937
Einzelheiten zu den Richtlinien 2937
Version der Richtlinie 2938
JSON-Richtliniendokument 2938
Weitere Informationen 2939
CloudWatchEventsBuiltInTargetExecutionAccess 2939
Diese Richtlinie wird verwendet 2939
Einzelheiten zu den Richtlinien 2939
Version der Richtlinie 2939
JSON-Richtliniendokument 2940
Weitere Informationen 2940

CloudWatchEventsFullAccess 2940
Diese Richtlinie wird verwendet 2941
Einzelheiten zu den Richtlinien 2941
Version der Richtlinie 2941
JSON-Richtliniendokument 2941
Weitere Informationen 2943
CloudWatchEventsInvocationAccess 2943
Diese Richtlinie wird verwendet 2943
Einzelheiten zu den Richtlinien 2944
Version der Richtlinie 2944
JSON-Richtliniendokument 2944
Weitere Informationen 2944
CloudWatchEventsReadOnlyAccess 2945
Diese Richtlinie wird verwendet 2945
Einzelheiten zu den Richtlinien 2945
Version der Richtlinie 2945
JSON-Richtliniendokument 2945
Weitere Informationen 2947
CloudWatchEventsServiceRolePolicy 2947
Diese Richtlinie wird verwendet 2947
Einzelheiten der Richtlinie 2947
Version der Richtlinie 2947
JSON-Richtliniendokument 2948
Weitere Informationen 2948
CloudWatchFullAccess 2948
Diese Richtlinie wird verwendet 2949
Einzelheiten zu den Richtlinien 2949
Version der Richtlinie 2949
JSON-Richtliniendokument 2949
Weitere Informationen 2950
CloudWatchFullAccessV2 2950
Diese Richtlinie wird verwendet 2950
Einzelheiten zu den Richtlinien 2951
Version der Richtlinie 2951
JSON-Richtliniendokument 2951
Weitere Informationen 2953

CloudWatchInternetMonitorServiceRolePolicy 2953
Diese Richtlinie wird verwendet 2953
Einzelheiten der Richtlinie 2953
Version der Richtlinie 2953
JSON-Richtliniendokument 2954
Weitere Informationen 2955
CloudWatchLambdaInsightsExecutionRolePolicy 2955
Diese Richtlinie wird verwendet 2955
Einzelheiten zu den Richtlinien 2955
Version der Richtlinie 2955
JSON-Richtliniendokument 2956
Weitere Informationen 2956
CloudWatchLogsCrossAccountSharingConfiguration 2956
Diese Richtlinie wird verwendet 2957
Einzelheiten zu den Richtlinien 2957
Version der Richtlinie 2957
JSON-Richtliniendokument 2957
Weitere Informationen 2958
CloudWatchLogsFullAccess 2958
Diese Richtlinie wird verwendet 2958
Einzelheiten zu den Richtlinien 2958
Version der Richtlinie 2959
JSON-Richtliniendokument 2959
Weitere Informationen 2959
CloudWatchLogsReadOnlyAccess 2960
Diese Richtlinie wird verwendet 2960
Einzelheiten zu den Richtlinien 2960
Version der Richtlinie 2960
JSON-Richtliniendokument 2960
Weitere Informationen 2961
CloudWatchNetworkMonitorServiceRolePolicy 2961
Diese Richtlinie wird verwendet 2961
Einzelheiten der Richtlinie 2961
Version der Richtlinie 2962
JSON-Richtliniendokument 2962
Weitere Informationen 2963

CloudWatchReadOnlyAccess 2963
Diese Richtlinie wird verwendet 2964
Einzelheiten zu den Richtlinien 2964
Version der Richtlinie 2964
JSON-Richtliniendokument 2964
Weitere Informationen 2966
CloudWatchSyntheticsFullAccess 2966
Diese Richtlinie wird verwendet 2966
Einzelheiten zu den Richtlinien 2966
Version der Richtlinie 2966
JSON-Richtliniendokument 2967
Weitere Informationen 2971
CloudWatchSyntheticsReadOnlyAccess 2971
Diese Richtlinie wird verwendet 2972
Einzelheiten zu den Richtlinien 2972
Version der Richtlinie 2972
JSON-Richtliniendokument 2972
Weitere Informationen 2973
ComprehendDataAccessRolePolicy 2973
Diese Richtlinie wird verwendet 2973
Einzelheiten zu den Richtlinien 2973
Version der Richtlinie 2973
JSON-Richtliniendokument 2974
Weitere Informationen 2974
ComprehendFullAccess 2974
Diese Richtlinie wird verwendet 2974
Einzelheiten zu den Richtlinien 2975
Version der Richtlinie 2975
JSON-Richtliniendokument 2975
Weitere Informationen 2975
ComprehendMedicalFullAccess 2976
Diese Richtlinie wird verwendet 2976
Einzelheiten zu den Richtlinien 2976
Version der Richtlinie 2976
JSON-Richtliniendokument 2976
Weitere Informationen 2977

ComprehendReadOnly 2977
Diese Richtlinie wird verwendet 2977
Einzelheiten zu den Richtlinien 2977
Version der Richtlinie 2977
JSON-Richtliniendokument 2978
Weitere Informationen 2979
ComputeOptimizerReadOnlyAccess 2979
Diese Richtlinie wird verwendet 2979
Einzelheiten zu den Richtlinien 2979
Version der Richtlinie 2980
JSON-Richtliniendokument 2980
Weitere Informationen 2981
ComputeOptimizerServiceRolePolicy 2981
Diese Richtlinie wird verwendet 2981
Einzelheiten der Richtlinie 2981
Version der Richtlinie 2982
JSON-Richtliniendokument 2982
Weitere Informationen 2983
ConfigConformsServiceRolePolicy 2983
Diese Richtlinie wird verwendet 2983
Einzelheiten der Richtlinie 2984
Version der Richtlinie 2984
JSON-Richtliniendokument 2984
Weitere Informationen 2987
CostOptimizationHubAdminAccess 2987
Diese Richtlinie wird verwendet 2987
Einzelheiten zu den Richtlinien 2987
Version der Richtlinie 2987
JSON-Richtliniendokument 2988
Weitere Informationen 2989
CostOptimizationHubReadOnlyAccess 2989
Diese Richtlinie wird verwendet 2989
Einzelheiten zu den Richtlinien 2989
Version der Richtlinie 2990
JSON-Richtliniendokument 2990
Weitere Informationen 2990

CostOptimizationHubServiceRolePolicy 2991
Diese Richtlinie wird verwendet 2991
Einzelheiten der Richtlinie 2991
Version der Richtlinie 2991
JSON-Richtliniendokument 2991
Weitere Informationen 2992
CustomerProfilesServiceLinkedRolePolicy 2992
Diese Richtlinie wird verwendet 2992
Einzelheiten der Richtlinie 2993
Version der Richtlinie 2993
JSON-Richtliniendokument 2993
Weitere Informationen 2994
DatabaseAdministrator 2994
Diese Richtlinie wird verwendet 2994
Einzelheiten zu den Richtlinien 2994
Version der Richtlinie 2994
JSON-Richtliniendokument 2995
Weitere Informationen 2997
DataScientist 2997
Diese Richtlinie wird verwendet 2997
Einzelheiten zu den Richtlinien 2997
Version der Richtlinie 2998
JSON-Richtliniendokument 2998
Weitere Informationen 3002
DAXServiceRolePolicy 3002
Diese Richtlinie wird verwendet 3002
Einzelheiten der Richtlinie 3002
Version der Richtlinie 3002
JSON-Richtliniendokument 3003
Weitere Informationen 3003
DynamoDBCloudWatchContributorInsightsServiceRolePolicy 3003
Diese Richtlinie wird verwendet 3004
Einzelheiten der Richtlinie 3004
Version der Richtlinie 3004
JSON-Richtliniendokument 3004
Weitere Informationen 3005

DynamoDBKinesisReplicationServiceRolePolicy 3005
Diese Richtlinie wird verwendet 3005
Einzelheiten der Richtlinie 3005
Version der Richtlinie 3005
JSON-Richtliniendokument 3006
Weitere Informationen 3006
DynamoDBReplicationServiceRolePolicy 3007
Diese Richtlinie wird verwendet 3007
Einzelheiten der Richtlinie 3007
Version der Richtlinie 3007
JSON-Richtliniendokument 3007
Weitere Informationen 3008
EC2FastLaunchFullAccess 3009
Diese Richtlinie wird verwendet 3009
Einzelheiten zu den Richtlinien 3009
Version der Richtlinie 3009
JSON-Richtliniendokument 3009
Weitere Informationen 3012
EC2FastLaunchServiceRolePolicy 3012
Diese Richtlinie wird verwendet 3012
Einzelheiten der Richtlinie 3013
Version der Richtlinie 3013
JSON-Richtliniendokument 3013
Weitere Informationen 3017
EC2FleetTimeShiftableServiceRolePolicy 3017
Diese Richtlinie wird verwendet 3017
Einzelheiten der Richtlinie 3017
Version der Richtlinie 3018
JSON-Richtliniendokument 3018
Weitere Informationen 3019
Ec2ImageBuilderCrossAccountDistributionAccess 3019
Diese Richtlinie wird verwendet 3020
Einzelheiten zu den Richtlinien 3020
Version der Richtlinie 3020
JSON-Richtliniendokument 3020
Weitere Informationen 3021

EC2ImageBuilderLifecycleExecutionPolicy 3021
Diese Richtlinie wird verwendet 3021
Einzelheiten zu den Richtlinien 3021
Version der Richtlinie 3021
JSON-Richtliniendokument 3022
Weitere Informationen 3024
EC2InstanceConnect 3024
Diese Richtlinie wird verwendet 3024
Einzelheiten zu den Richtlinien 3024
Version der Richtlinie 3024
JSON-Richtliniendokument 3025
Weitere Informationen 3025
Ec2InstanceConnectEndpoint 3025
Diese Richtlinie wird verwendet 3025
Einzelheiten der Richtlinie 3026
Version der Richtlinie 3026
JSON-Richtliniendokument 3026
Weitere Informationen 3028
EC2InstanceProfileForImageBuilder 3028
Diese Richtlinie wird verwendet 3028
Einzelheiten zu den Richtlinien 3028
Version der Richtlinie 3029
JSON-Richtliniendokument 3029
Weitere Informationen 3030
EC2InstanceProfileForImageBuilderECRContainerBuilds 3030
Diese Richtlinie wird verwendet 3030
Einzelheiten zu den Richtlinien 3030
Version der Richtlinie 3031
JSON-Richtliniendokument 3031
Weitere Informationen 3032
ECRReplicationServiceRolePolicy 3032
Diese Richtlinie wird verwendet 3033
Einzelheiten der Richtlinie 3033
Version der Richtlinie 3033
JSON-Richtliniendokument 3033
Weitere Informationen 3034

ElastiCacheServiceRolePolicy 3034
Diese Richtlinie wird verwendet 3034
Einzelheiten der Richtlinie 3034
Version der Richtlinie 3034
JSON-Richtliniendokument 3035
Weitere Informationen 3037
ElasticLoadBalancingFullAccess 3037
Diese Richtlinie wird verwendet 3037
Einzelheiten zu den Richtlinien 3037
Version der Richtlinie 3037
JSON-Richtliniendokument 3038
Weitere Informationen 3039
ElasticLoadBalancingReadOnly 3039
Diese Richtlinie wird verwendet 3039
Einzelheiten zu den Richtlinien 3039
Version der Richtlinie 3040
JSON-Richtliniendokument 3040
Weitere Informationen 3041
ElementalActivationsDownloadSoftwareAccess 3041
Diese Richtlinie wird verwendet 3041
Einzelheiten zu den Richtlinien 3041
Version der Richtlinie 3042
JSON-Richtliniendokument 3042
Weitere Informationen 3042
ElementalActivationsFullAccess 3042
Diese Richtlinie wird verwendet 3043
Einzelheiten zu den Richtlinien 3043
Version der Richtlinie 3043
JSON-Richtliniendokument 3043
Weitere Informationen 3043
ElementalActivationsGenerateLicenses 3044
Diese Richtlinie wird verwendet 3044
Einzelheiten zu den Richtlinien 3044
Version der Richtlinie 3044
JSON-Richtliniendokument 3044
Weitere Informationen 3045

ElementalActivationsReadOnlyAccess 3045
Diese Richtlinie wird verwendet 3045
Einzelheiten zu den Richtlinien 3045
Version der Richtlinie 3046
JSON-Richtliniendokument 3046
Weitere Informationen 3046
ElementalAppliancesSoftwareFullAccess 3046
Diese Richtlinie wird verwendet 3047
Einzelheiten zu den Richtlinien 3047
Version der Richtlinie 3047
JSON-Richtliniendokument 3047
Weitere Informationen 3048
ElementalAppliancesSoftwareReadOnlyAccess 3048
Diese Richtlinie wird verwendet 3048
Einzelheiten zu den Richtlinien 3048
Version der Richtlinie 3048
JSON-Richtliniendokument 3049
Weitere Informationen 3049
ElementalSupportCenterFullAccess 3049
Diese Richtlinie wird verwendet 3049
Einzelheiten zu den Richtlinien 3049
Version der Richtlinie 3050
JSON-Richtliniendokument 3050
Weitere Informationen 3050
EMRDescribeClusterPolicyForEMRWAL 3051
Diese Richtlinie wird verwendet 3051
Einzelheiten der Richtlinie 3051
Version der Richtlinie 3051
JSON-Richtliniendokument 3051
Weitere Informationen 3052
FMSServiceRolePolicy 3052
Diese Richtlinie wird verwendet 3052
Einzelheiten der Richtlinie 3052
Version der Richtlinie 3052
JSON-Richtliniendokument 3053
Weitere Informationen 3069

FSxDeleteServiceLinkedRoleAccess 3069
Diese Richtlinie wird verwendet 3069
Einzelheiten der Richtlinie 3069
Version der Richtlinie 3069
JSON-Richtliniendokument 3070
Weitere Informationen 3070
GameLiftGameServerGroupPolicy 3070
Diese Richtlinie wird verwendet 3070
Einzelheiten zu den Richtlinien 3071
Version der Richtlinie 3071
JSON-Richtliniendokument 3071
Weitere Informationen 3073
GlobalAcceleratorFullAccess 3073
Diese Richtlinie wird verwendet 3073
Einzelheiten zu den Richtlinien 3073
Version der Richtlinie 3073
JSON-Richtliniendokument 3074
Weitere Informationen 3075
GlobalAcceleratorReadOnlyAccess 3075
Diese Richtlinie wird verwendet 3075
Einzelheiten zu den Richtlinien 3075
Version der Richtlinie 3075
JSON-Richtliniendokument 3076
Weitere Informationen 3076
GreengrassOTAUpdateArtifactAccess 3076
Diese Richtlinie wird verwendet 3076
Einzelheiten zu den Richtlinien 3076
Version der Richtlinie 3077
JSON-Richtliniendokument 3077
Weitere Informationen 3077
GroundTruthSyntheticConsoleFullAccess 3078
Diese Richtlinie wird verwendet 3078
Einzelheiten zu den Richtlinien 3078
Version der Richtlinie 3078
JSON-Richtliniendokument 3078
Weitere Informationen 3079

GroundTruthSyntheticConsoleReadOnlyAccess 3079
Diese Richtlinie wird verwendet 3079
Einzelheiten zu den Richtlinien 3079
Version der Richtlinie 3080
JSON-Richtliniendokument 3080
Weitere Informationen 3080
Health_OrganizationsServiceRolePolicy 3080
Diese Richtlinie wird verwendet 3081
Einzelheiten der Richtlinie 3081
Version der Richtlinie 3081
JSON-Richtliniendokument 3081
Weitere Informationen 3082
IAMAccessAdvisorReadOnly 3082
Diese Richtlinie wird verwendet 3082
Einzelheiten zu den Richtlinien 3082
Version der Richtlinie 3082
JSON-Richtliniendokument 3083
Weitere Informationen 3083
IAMAccessAnalyzerFullAccess 3084
Diese Richtlinie wird verwendet 3084
Einzelheiten zu den Richtlinien 3084
Version der Richtlinie 3084
JSON-Richtliniendokument 3084
Weitere Informationen 3085
IAMAccessAnalyzerReadOnlyAccess 3086
Diese Richtlinie wird verwendet 3086
Einzelheiten zu den Richtlinien 3086
Version der Richtlinie 3086
JSON-Richtliniendokument 3086
Weitere Informationen 3087
IAMFullAccess 3087
Diese Richtlinie wird verwendet 3087
Einzelheiten zu den Richtlinien 3087
Version der Richtlinie 3087
JSON-Richtliniendokument 3088
Weitere Informationen 3088

IAMReadOnlyAccess 3088
Diese Richtlinie wird verwendet 3089
Einzelheiten zu den Richtlinien 3089
Version der Richtlinie 3089
JSON-Richtliniendokument 3089
Weitere Informationen 3090
IAMSelfManageServiceSpecificCredentials 3090
Diese Richtlinie wird verwendet 3090
Einzelheiten zu den Richtlinien 3090
Version der Richtlinie 3090
JSON-Richtliniendokument 3091
Weitere Informationen 3091
IAMUserChangePassword 3091
Diese Richtlinie wird verwendet 3092
Einzelheiten zu den Richtlinien 3092
Version der Richtlinie 3092
JSON-Richtliniendokument 3092
Weitere Informationen 3093
IAMUserSSHKeys 3093
Diese Richtlinie wird verwendet 3093
Einzelheiten zu den Richtlinien 3093
Version der Richtlinie 3093
JSON-Richtliniendokument 3094
Weitere Informationen 3094
IVSFullAccess 3094
Diese Richtlinie wird verwendet 3095
Einzelheiten zu den Richtlinien 3095
Version der Richtlinie 3095
JSON-Richtliniendokument 3095
Weitere Informationen 3096
IVSReadOnlyAccess 3096
Diese Richtlinie wird verwendet 3096
Einzelheiten zu den Richtlinien 3096
Version der Richtlinie 3096
JSON-Richtliniendokument 3097
Weitere Informationen 3098

IVSRecordToS3 3098
Diese Richtlinie wird verwendet 3098
Einzelheiten der Richtlinie 3098
Version der Richtlinie 3098
JSON-Richtliniendokument 3099
Weitere Informationen 3099
KafkaConnectServiceRolePolicy 3099
Diese Richtlinie wird verwendet 3099
Einzelheiten der Richtlinie 3099
Version der Richtlinie 3100
JSON-Richtliniendokument 3100
Weitere Informationen 3101
KafkaServiceRolePolicy 3102
Diese Richtlinie wird verwendet 3102
Einzelheiten der Richtlinie 3102
Version der Richtlinie 3102
JSON-Richtliniendokument 3102
Weitere Informationen 3104
KeyspacesReplicationServiceRolePolicy 3104
Diese Richtlinie wird verwendet 3104
Einzelheiten der Richtlinie 3104
Version der Richtlinie 3104
JSON-Richtliniendokument 3105
Weitere Informationen 3105
LakeFormationDataAccessServiceRolePolicy 3105
Diese Richtlinie wird verwendet 3105
Einzelheiten der Richtlinie 3106
Version der Richtlinie 3106
JSON-Richtliniendokument 3106
Weitere Informationen 3106
LexBotPolicy 3107
Diese Richtlinie wird verwendet 3107
Einzelheiten der Richtlinie 3107
Version der Richtlinie 3107
JSON-Richtliniendokument 3107
Weitere Informationen 3108

LexChannelPolicy 3108
Diese Richtlinie wird verwendet 3108
Einzelheiten der Richtlinie 3108
Version der Richtlinie 3109
JSON-Richtliniendokument 3109
Weitere Informationen 3109
LightsailExportAccess 3109
Diese Richtlinie wird verwendet 3110
Einzelheiten der Richtlinie 3110
Version der Richtlinie 3110
JSON-Richtliniendokument 3110
Weitere Informationen 3111
MediaConnectGatewayInstanceRolePolicy 3111
Diese Richtlinie wird verwendet 3111
Einzelheiten zu den Richtlinien 3111
Version der Richtlinie 3112
JSON-Richtliniendokument 3112
Weitere Informationen 3112
MediaPackageServiceRolePolicy 3113
Diese Richtlinie wird verwendet 3113
Einzelheiten der Richtlinie 3113
Version der Richtlinie 3113
JSON-Richtliniendokument 3113
Weitere Informationen 3114
MemoryDBServiceRolePolicy 3114
Diese Richtlinie wird verwendet 3114
Einzelheiten der Richtlinie 3114
Version der Richtlinie 3115
JSON-Richtliniendokument 3115
Weitere Informationen 3117
MigrationHubDMSAccessServiceRolePolicy 3117
Diese Richtlinie wird verwendet 3117
Einzelheiten der Richtlinie 3117
Version der Richtlinie 3117
JSON-Richtliniendokument 3118
Weitere Informationen 3118

MigrationHubServiceRolePolicy 3119
Diese Richtlinie wird verwendet 3119
Einzelheiten der Richtlinie 3119
Version der Richtlinie 3119
JSON-Richtliniendokument 3119
Weitere Informationen 3121
MigrationHubSMSAccessServiceRolePolicy 3121
Diese Richtlinie wird verwendet 3121
Einzelheiten der Richtlinie 3121
Version der Richtlinie 3121
JSON-Richtliniendokument 3122
Weitere Informationen 3123
MonitronServiceRolePolicy 3123
Diese Richtlinie wird verwendet 3123
Einzelheiten der Richtlinie 3123
Version der Richtlinie 3123
JSON-Richtliniendokument 3124
Weitere Informationen 3124
NeptuneConsoleFullAccess 3124
Diese Richtlinie wird verwendet 3125
Einzelheiten zu den Richtlinien 3125
Version der Richtlinie 3125
JSON-Richtliniendokument 3125
Weitere Informationen 3131
NeptuneFullAccess 3131
Diese Richtlinie wird verwendet 3131
Einzelheiten zu den Richtlinien 3131
Version der Richtlinie 3131
JSON-Richtliniendokument 3132
Weitere Informationen 3135
NeptuneGraphReadOnlyAccess 3136
Diese Richtlinie wird verwendet 3136
Einzelheiten zu den Richtlinien 3136
Version der Richtlinie 3136
JSON-Richtliniendokument 3136
Weitere Informationen 3138

NeptuneReadOnlyAccess 3138
Diese Richtlinie wird verwendet 3138
Einzelheiten zu den Richtlinien 3138
Version der Richtlinie 3139
JSON-Richtliniendokument 3139
Weitere Informationen 3141
NetworkAdministrator 3141
Diese Richtlinie wird verwendet 3141
Einzelheiten zu den Richtlinien 3142
Version der Richtlinie 3142
JSON-Richtliniendokument 3142
Weitere Informationen 3148
OAMFullAccess 3149
Diese Richtlinie wird verwendet 3149
Einzelheiten zu den Richtlinien 3149
Version der Richtlinie 3149
JSON-Richtliniendokument 3149
Weitere Informationen 3150
OAMReadOnlyAccess 3150
Diese Richtlinie wird verwendet 3150
Einzelheiten zu den Richtlinien 3150
Version der Richtlinie 3150
JSON-Richtliniendokument 3151
Weitere Informationen 3151
OpensearchIngestionSelfManagedVpcePolicy 3151
Diese Richtlinie wird verwendet 3152
Einzelheiten der Richtlinie 3152
Version der Richtlinie 3152
JSON-Richtliniendokument 3152
Weitere Informationen 3153
PartnerCentralAccountManagementUserRoleAssociation 3153
Diese Richtlinie wird verwendet 3153
Einzelheiten zu den Richtlinien 3153
Version der Richtlinie 3154
JSON-Richtliniendokument 3154
Weitere Informationen 3155

PowerUserAccess 3155
Diese Richtlinie wird verwendet 3155
Einzelheiten zu den Richtlinien 3155
Version der Richtlinie 3155
JSON-Richtliniendokument 3156
Weitere Informationen 3156
QBusinessServiceRolePolicy 3157
Diese Richtlinie wird verwendet 3157
Einzelheiten der Richtlinie 3157
Version der Richtlinie 3157
JSON-Richtliniendokument 3157
Weitere Informationen 3159
QuickSightAccessForS3StorageManagementAnalyticsReadOnly 3159
Diese Richtlinie wird verwendet 3159
Einzelheiten zu den Richtlinien 3159
Version der Richtlinie 3160
JSON-Richtliniendokument 3160
Weitere Informationen 3160
RDSCloudHsmAuthorizationRole 3161
Diese Richtlinie wird verwendet 3161
Einzelheiten zu den Richtlinien 3161
Version der Richtlinie 3161
JSON-Richtliniendokument 3161
Weitere Informationen 3162
ReadOnlyAccess 3162
Diese Richtlinie wird verwendet 3162
Einzelheiten zu den Richtlinien 3162
Version der Richtlinie 3163
JSON-Richtliniendokument 3163
Weitere Informationen 3212
ResourceGroupsandTagEditorFullAccess 3212
Diese Richtlinie wird verwendet 3213
Einzelheiten zu den Richtlinien 3213
Version der Richtlinie 3213
JSON-Richtliniendokument 3213
Weitere Informationen 3214

ResourceGroupsandTagEditorReadOnlyAccess 3214
Diese Richtlinie wird verwendet 3214
Einzelheiten zu den Richtlinien 3214
Version der Richtlinie 3214
JSON-Richtliniendokument 3215
Weitere Informationen 3215
ResourceGroupsServiceRolePolicy 3215
Diese Richtlinie wird verwendet 3216
Einzelheiten der Richtlinie 3216
Version der Richtlinie 3216
JSON-Richtliniendokument 3216
Weitere Informationen 3217
ROSAAmazonEBSCSIDriverOperatorPolicy 3217
Diese Richtlinie wird verwendet 3217
Einzelheiten zu den Richtlinien 3217
Version der Richtlinie 3217
JSON-Richtliniendokument 3218
Weitere Informationen 3220
ROSACloudNetworkConfigOperatorPolicy 3221
Diese Richtlinie wird verwendet 3221
Einzelheiten zu den Richtlinien 3221
Version der Richtlinie 3221
JSON-Richtliniendokument 3222
Weitere Informationen 3222
ROSAControlPlaneOperatorPolicy 3223
Diese Richtlinie wird verwendet 3223
Einzelheiten zu den Richtlinien 3223
Version der Richtlinie 3223
JSON-Richtliniendokument 3223
Weitere Informationen 3228
ROSAImageRegistryOperatorPolicy 3228
Diese Richtlinie wird verwendet 3228
Einzelheiten zu den Richtlinien 3228
Version der Richtlinie 3229
JSON-Richtliniendokument 3229
Weitere Informationen 3230

ROSAIngressOperatorPolicy 3230
Diese Richtlinie wird verwendet 3230
Einzelheiten zu den Richtlinien 3231
Version der Richtlinie 3231
JSON-Richtliniendokument 3231
Weitere Informationen 3232
ROSAInstallerPolicy 3232
Diese Richtlinie wird verwendet 3232
Einzelheiten zu den Richtlinien 3232
Version der Richtlinie 3233
JSON-Richtliniendokument 3233
Weitere Informationen 3241
ROSAKMSProviderPolicy 3241
Diese Richtlinie wird verwendet 3241
Einzelheiten zu den Richtlinien 3241
Version der Richtlinie 3241
JSON-Richtliniendokument 3242
Weitere Informationen 3242
ROSAKubeControllerPolicy 3242
Diese Richtlinie wird verwendet 3243
Einzelheiten zu den Richtlinien 3243
Version der Richtlinie 3243
JSON-Richtliniendokument 3243
Weitere Informationen 3247
ROSAManageSubscription 3248
Diese Richtlinie wird verwendet 3248
Einzelheiten zu den Richtlinien 3248
Version der Richtlinie 3248
JSON-Richtliniendokument 3248
Weitere Informationen 3249
ROSANodePoolManagementPolicy 3249
Diese Richtlinie wird verwendet 3250
Einzelheiten zu den Richtlinien 3250
Version der Richtlinie 3250
JSON-Richtliniendokument 3250
Weitere Informationen 3256

ROSASRESupportPolicy 3256
Diese Richtlinie wird verwendet 3256
Einzelheiten zu den Richtlinien 3256
Version der Richtlinie 3257
JSON-Richtliniendokument 3257
Weitere Informationen 3262
ROSAWorkerInstancePolicy 3262
Diese Richtlinie wird verwendet 3262
Einzelheiten zu den Richtlinien 3262
Version der Richtlinie 3262
JSON-Richtliniendokument 3263
Weitere Informationen 3263
Route53RecoveryReadinessServiceRolePolicy 3263
Diese Richtlinie wird verwendet 3263
Einzelheiten der Richtlinie 3264
Version der Richtlinie 3264
JSON-Richtliniendokument 3264
Weitere Informationen 3267
Route53ResolverServiceRolePolicy 3268
Diese Richtlinie wird verwendet 3268
Einzelheiten der Richtlinie 3268
Version der Richtlinie 3268
JSON-Richtliniendokument 3268
Weitere Informationen 3269
S3StorageLensServiceRolePolicy 3269
Diese Richtlinie wird verwendet 3269
Einzelheiten der Richtlinie 3269
Version der Richtlinie 3270
JSON-Richtliniendokument 3270
Weitere Informationen 3270
SecretsManagerReadWrite 3271
Diese Richtlinie wird verwendet 3271
Einzelheiten zu den Richtlinien 3271
Version der Richtlinie 3271
JSON-Richtliniendokument 3271
Weitere Informationen 3273

SecurityAudit 3273
Diese Richtlinie wird verwendet 3273
Einzelheiten zu den Richtlinien 3273
Version der Richtlinie 3274
JSON-Richtliniendokument 3274
Weitere Informationen 3291
SecurityLakeServiceLinkedRole 3291
Diese Richtlinie wird verwendet 3291
Einzelheiten der Richtlinie 3292
Version der Richtlinie 3292
JSON-Richtliniendokument 3292
Weitere Informationen 3295
ServerMigration_ServiceRole 3295
Diese Richtlinie wird verwendet 3295
Einzelheiten zu den Richtlinien 3295
Version der Richtlinie 3296
JSON-Richtliniendokument 3296
Weitere Informationen 3301
ServerMigrationConnector 3301
Diese Richtlinie wird verwendet 3301
Einzelheiten zu den Richtlinien 3301
Version der Richtlinie 3301
JSON-Richtliniendokument 3302
Weitere Informationen 3303
ServerMigrationServiceConsoleFullAccess 3303
Diese Richtlinie wird verwendet 3304
Einzelheiten zu den Richtlinien 3304
Version der Richtlinie 3304
JSON-Richtliniendokument 3304
Weitere Informationen 3306
ServerMigrationServiceLaunchRole 3306
Diese Richtlinie wird verwendet 3306
Einzelheiten zu den Richtlinien 3306
Version der Richtlinie 3306
JSON-Richtliniendokument 3307
Weitere Informationen 3309

ServerMigrationServiceRoleForInstanceValidation 3310
Diese Richtlinie wird verwendet 3310
Einzelheiten zu den Richtlinien 3310
Version der Richtlinie 3310
JSON-Richtliniendokument 3310
Weitere Informationen 3311
ServiceQuotasFullAccess 3311
Diese Richtlinie wird verwendet 3311
Einzelheiten zu den Richtlinien 3311
Version der Richtlinie 3311
JSON-Richtliniendokument 3312
Weitere Informationen 3313
ServiceQuotasReadOnlyAccess 3314
Diese Richtlinie wird verwendet 3314
Einzelheiten zu den Richtlinien 3314
Version der Richtlinie 3314
JSON-Richtliniendokument 3314
Weitere Informationen 3315
ServiceQuotasServiceRolePolicy 3316
Diese Richtlinie wird verwendet 3316
Einzelheiten der Richtlinie 3316
Version der Richtlinie 3316
JSON-Richtliniendokument 3316
Weitere Informationen 3317
SimpleWorkflowFullAccess 3317
Diese Richtlinie wird verwendet 3317
Einzelheiten zu den Richtlinien 3317
Version der Richtlinie 3317
JSON-Richtliniendokument 3318
Weitere Informationen 3318
SplitCostAllocationDataServiceRolePolicy 3318
Diese Richtlinie wird verwendet 3318
Einzelheiten der Richtlinie 3319
Version der Richtlinie 3319
JSON-Richtliniendokument 3319
Weitere Informationen 3320

SupportUser 3320
Diese Richtlinie wird verwendet 3320
Einzelheiten zu den Richtlinien 3320
Version der Richtlinie 3320
JSON-Richtliniendokument 3321
Weitere Informationen 3326
SystemAdministrator 3326
Diese Richtlinie wird verwendet 3326
Einzelheiten zu den Richtlinien 3326
Version der Richtlinie 3326
JSON-Richtliniendokument 3327
Weitere Informationen 3333
TranslateFullAccess 3333
Diese Richtlinie wird verwendet 3333
Einzelheiten zu den Richtlinien 3333
Version der Richtlinie 3333
JSON-Richtliniendokument 3334
Weitere Informationen 3334
TranslateReadOnly 3334
Diese Richtlinie wird verwendet 3335
Einzelheiten zu den Richtlinien 3335
Version der Richtlinie 3335
JSON-Richtliniendokument 3335
Weitere Informationen 3336
ViewOnlyAccess 3336
Diese Richtlinie wird verwendet 3336
Einzelheiten zu den Richtlinien 3336
Version der Richtlinie 3336
JSON-Richtliniendokument 3337
Weitere Informationen 3345
VMImportExportRoleForAWSConnector 3345
Diese Richtlinie wird verwendet 3346
Einzelheiten zu den Richtlinien 3346
Version der Richtlinie 3346
JSON-Richtliniendokument 3346
Weitere Informationen 3347

VPCLatticeFullAccess 3347
Diese Richtlinie wird verwendet 3347
Einzelheiten zu den Richtlinien 3347
Version der Richtlinie 3348
JSON-Richtliniendokument 3348
Weitere Informationen 3350
VPCLatticeReadOnlyAccess 3350
Diese Richtlinie wird verwendet 3350
Einzelheiten zu den Richtlinien 3350
Version der Richtlinie 3351
JSON-Richtliniendokument 3351
Weitere Informationen 3352
VPCLatticeServicesInvokeAccess 3352
Diese Richtlinie wird verwendet 3352
Einzelheiten zu den Richtlinien 3352
Version der Richtlinie 3352
JSON-Richtliniendokument 3353
Weitere Informationen 3353
WAFLoggingServiceRolePolicy 3353
Diese Richtlinie wird verwendet 3353
Einzelheiten der Richtlinie 3353
Version der Richtlinie 3354
JSON-Richtliniendokument 3354
Weitere Informationen 3354
WAFRegionalLoggingServiceRolePolicy 3354
Diese Richtlinie wird verwendet 3355
Einzelheiten der Richtlinie 3355
Version der Richtlinie 3355
JSON-Richtliniendokument 3355
Weitere Informationen 3356
WAFV2LoggingServiceRolePolicy 3356
Diese Richtlinie wird verwendet 3356
Einzelheiten der Richtlinie 3356
Version der Richtlinie 3356
JSON-Richtliniendokument 3357
Weitere Informationen 3357

WellArchitectedConsoleFullAccess 3357
Diese Richtlinie wird verwendet 3358
Einzelheiten zu den Richtlinien 3358
Version der Richtlinie 3358
JSON-Richtliniendokument 3358
Weitere Informationen 3358
WellArchitectedConsoleReadOnlyAccess 3359
Diese Richtlinie wird verwendet 3359
Einzelheiten zu den Richtlinien 3359
Version der Richtlinie 3359
JSON-Richtliniendokument 3359
Weitere Informationen 3360
WorkLinkServiceRolePolicy 3360
Diese Richtlinie wird verwendet 3360
Einzelheiten zu den Richtlinien 3360
Version der Richtlinie 3361
JSON-Richtliniendokument 3361
Weitere Informationen 3361
..... mmmccclxiii

Was sind -AWSverwaltete Richtlinien?

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wirdAWS. AWS Von verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele häufige Anwendungsfälle bereitstellen. Sie erleichtern Ihnen den Einstieg in die Zuweisung von Berechtigungen für Benutzer, Gruppen und Rollen, als ob Sie die Richtlinien selbst schreiben müssten.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise keine Berechtigungen mit den geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich die Aktualisierung auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für vorhandene Services verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Grundlegendes zu Richtlinienreferenzseiten

Jede Richtlinienreferenzseite enthält die folgenden Informationen:

- Verwenden dieser Richtlinie – Ob Sie die Richtlinie an Benutzer, Gruppen und Rollen anfügen können
- Richtliniendetails
  - Typ – Der Typ der AWS verwalteten Richtlinie
    - `AWS managed policy` – Eine AWS verwaltete Standardrichtlinie
    - `Job function policy` – Richtlinie, die auf gängige Job-Funktionen in der Branche abgestimmt ist
    - `Service-linked role policy` – Richtlinie, die einer serviceverknüpften Rolle zugeordnet ist, die es einem Service ermöglicht, Aktionen in Ihrem Namen auszuführen, z. B. the section called “AmazonRDSPreviewServiceRolePolicy”

    - `Service role policy` – Richtlinie, die für die Arbeit mit Servicerollen entwickelt wurde, z. B. the section called “AWSControlTowerServiceRolePolicy”
  - Erstellungszeit – wann die Richtlinie zum ersten Mal erstellt wurde
  - Bearbeitungszeit – Wann diese Version der Richtlinie bearbeitet wurde
  - ARN – Der Amazon-Ressourcenname der Richtlinie
- Richtlinienversion – Die Version der Berechtigungen, die von der Richtlinie gewährt werden
- JSON-Richtliniendokument – Die JSON-Richtlinie
- Weitere Informationen – Links zur Dokumentation im Zusammenhang mit von AWS verwalteten Richtlinien

Veraltete, von AWS verwaltete Richtlinien

AWS aktualisiert regelmäßig AWS verwaltete Richtlinien. In den meisten Fällen fügen wir einer Richtlinie Berechtigungen hinzu. Dies geschieht, wenn wir einen neuen Service oder eine neue Funktion starten. Um die Sicherheit AWS verwalteter Richtlinien zu verbessern, reduzieren wir manchmal den Geltungsbereich von Richtlinien. Wenn wir Berechtigungen aus einer Richtlinie entfernen, setzen wir die Richtlinie auf einen veralteten Status und machen einen neuen verfügbar. Wenn einen Service oder ein Feature AWS als veraltet einstuft, wird auch die AWS von verwaltete Richtlinie für dieses Feature als veraltet eingestuft.

Wenn Sie eine E-Mail-Benachrichtigung erhalten, dass eine von Ihnen verwendete Richtlinie veraltet ist, empfehlen wir Ihnen, sofort Maßnahmen zu ergreifen. Identifizieren Sie die Änderung der Richtlinie und aktualisieren Sie Ihre Workflows. Wenn eine Ersatzrichtlinie AWS bereitstellt, planen Sie, sie allen betroffenen Identitäten (Benutzer, Gruppen und Rollen) anzufügen und dann die veraltete Richtlinie von diesen Identitäten zu trennen.

Eine veraltete Richtlinie hat folgende Merkmale:

- Es wird aus diesem Handbuch entfernt.
- Berechtigungen funktionieren weiterhin für alle derzeit angefügten Identitäten.
- In Konten, in denen die Richtlinie an eine Identität angefügt ist, wird sie in der Liste Richtlinien in der IAM-Konsole mit einem Warnsymbol daneben angezeigt.
- Sie kann keinen neuen Identitäten zugeordnet werden. Wenn Sie sie von einer aktuellen Identität trennen, können Sie sie nicht erneut anfügen.
- Nachdem Sie es von allen aktuellen Entitäten getrennt haben, ist es nicht mehr sichtbar.

AWS verwaltete Richtlinien

AWS verwaltete Richtlinien

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

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

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

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

- AmazonEC2ContainerServiceforEC2Role
- AmazonEC2ContainerServiceRole
- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- AmazonEC2RoleforAWSCodeDeploy
- AmazonEC2RoleforAWSCodeDeployLimited
- AmazonEC2RoleforDataPipelineRole
- AmazonEC2RoleforSSM
- AmazonEC2RolePolicyForLaunchWizard
- AmazonEC2SpotFleetAutoscaleRole
- AmazonEC2SpotFleetTaggingRole
- AmazonECS_FullAccess
- AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
- AmazonECSInfrastructureRolePolicyForVolumes
- AmazonECSServiceRolePolicy
- AmazonECSTaskExecutionRolePolicy
- AmazonEFSCSIDriverPolicy
- AmazonEKS_CNI_Policy
- AmazonEKSClusterPolicy
- AmazonEKSConnectorServiceRolePolicy
- AmazonEKSFargatePodExecutionRolePolicy
- AmazonEKSForFargateServiceRolePolicy
- AmazonEKSLocalOutpostClusterPolicy
- AmazonEKSLocalOutpostServiceRolePolicy
- AmazonEKSServicePolicy
- AmazonEKSServiceRolePolicy
- AmazonEKSVPCResourceController
- AmazonEKSWorkerNodePolicy
- AmazonElastiCacheFullAccess

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

- AmazonESCognitoAccess
- AmazonESFullAccess
- AmazonESReadOnlyAccess
- AmazonEventBridgeApiDestinationsServiceRolePolicy
- AmazonEventBridgeFullAccess
- AmazonEventBridgePipesFullAccess
- AmazonEventBridgePipesOperatorAccess
- AmazonEventBridgePipesReadOnlyAccess
- AmazonEventBridgeReadOnlyAccess
- AmazonEventBridgeSchedulerFullAccess
- AmazonEventBridgeSchedulerReadOnlyAccess
- AmazonEventBridgeSchemasFullAccess
- AmazonEventBridgeSchemasReadOnlyAccess
- AmazonEventBridgeSchemasServiceRolePolicy
- AmazonFISServiceRolePolicy
- AmazonForecastFullAccess
- AmazonFraudDetectorFullAccessPolicy
- AmazonFreeRTOSFullAccess
- AmazonFreeRTOSOTAUpdate
- AmazonFSxConsoleFullAccess
- AmazonFSxConsoleReadOnlyAccess
- AmazonFSxFullAccess
- AmazonFSxReadOnlyAccess
- AmazonFSxServiceRolePolicy
- AmazonGlacierFullAccess
- AmazonGlacierReadOnlyAccess
- AmazonGrafanaAthenaAccess
- AmazonGrafanaCloudWatchAccess
- AmazonGrafanaRedshiftAccess

- AmazonGrafanaServiceLinkedRolePolicy
- AmazonGuardDutyFullAccess
- AmazonGuardDutyMalwareProtectionServiceRolePolicy
- AmazonGuardDutyReadOnlyAccess
- AmazonGuardDutyServiceRolePolicy
- AmazonHealthLakeFullAccess
- AmazonHealthLakeReadOnlyAccess
- AmazonHoneycodeFullAccess
- AmazonHoneycodeReadOnlyAccess
- AmazonHoneycodeServiceRolePolicy
- AmazonHoneycodeTeamAssociationFullAccess
- AmazonHoneycodeTeamAssociationReadOnlyAccess
- AmazonHoneycodeWorkbookFullAccess
- AmazonHoneycodeWorkbookReadOnlyAccess
- AmazonInspector2AgentlessServiceRolePolicy
- AmazonInspector2FullAccess
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ReadOnlyAccess
- AmazonInspector2ServiceRolePolicy
- AmazonInspectorFullAccess
- AmazonInspectorReadOnlyAccess
- AmazonInspectorServiceRolePolicy
- AmazonKendraFullAccess
- AmazonKendraReadOnlyAccess
- AmazonKeyspacesFullAccess
- AmazonKeyspacesReadOnlyAccess
- AmazonKeyspacesReadOnlyAccess_v2
- AmazonKinesisAnalyticsFullAccess
- AmazonKinesisAnalyticsReadOnly

- AmazonKinesisFirehoseFullAccess
- AmazonKinesisFirehoseReadOnlyAccess
- AmazonKinesisFullAccess
- AmazonKinesisReadOnlyAccess
- AmazonKinesisVideoStreamsFullAccess
- AmazonKinesisVideoStreamsReadOnlyAccess
- AmazonLaunchWizard_Fullaccess
- AmazonLaunchWizardFullAccessV2
- AmazonLexChannelsAccess
- AmazonLexFullAccess
- AmazonLexReadOnly
- AmazonLexReplicationPolicy
- AmazonLexRunBotsOnly
- AmazonLexV2BotPolicy
- AmazonLookoutEquipmentFullAccess
- AmazonLookoutEquipmentReadOnlyAccess
- AmazonLookoutMetricsFullAccess
- AmazonLookoutMetricsReadOnlyAccess
- AmazonLookoutVisionConsoleFullAccess
- AmazonLookoutVisionConsoleReadOnlyAccess
- AmazonLookoutVisionFullAccess
- AmazonLookoutVisionReadOnlyAccess
- AmazonMachineLearningBatchPredictionsAccess
- AmazonMachineLearningCreateOnlyAccess
- AmazonMachineLearningFullAccess
- AmazonMachineLearningManageRealTimeEndpointOnlyAccess
- AmazonMachineLearningReadOnlyAccess
- AmazonMachineLearningRealTimePredictionOnlyAccess
- AmazonMachineLearningRoleforRedshiftDataSourceV3

- AmazonMacieFullAccess
- AmazonMacieHandshakeRole
- AmazonMacieReadOnlyAccess
- AmazonMacieServiceRole
- AmazonMacieServiceRolePolicy
- AmazonManagedBlockchainConsoleFullAccess
- AmazonManagedBlockchainFullAccess
- AmazonManagedBlockchainReadOnlyAccess
- AmazonManagedBlockchainServiceRolePolicy
- AmazonMCSFullAccess
- AmazonMCSReadOnlyAccess
- AmazonMechanicalTurkFullAccess
- AmazonMechanicalTurkReadOnly
- AmazonMemoryDBFullAccess
- AmazonMemoryDBReadOnlyAccess
- AmazonMobileAnalyticsFinancialReportAccess
- AmazonMobileAnalyticsFullAccess
- AmazonMobileAnalyticsNon-financialReportAccess
- AmazonMobileAnalyticsWriteOnlyAccess
- AmazonMonitronFullAccess
- AmazonMQApiFullAccess
- AmazonMQApiReadOnlyAccess
- AmazonMQFullAccess
- AmazonMQReadOnlyAccess
- AmazonMQServiceRolePolicy
- AmazonMSKConnectReadOnlyAccess
- AmazonMSKFullAccess
- AmazonMSKReadOnlyAccess
- AmazonMWAAServiceRolePolicy

- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser
- AmazonOmicsFullAccess
- AmazonOmicsReadOnlyAccess
- AmazonOneEnterpriseFullAccess
- AmazonOneEnterpriseInstallerAccess
- AmazonOneEnterpriseReadOnlyAccess
- AmazonOpenSearchDashboardsServiceRolePolicy
- AmazonOpenSearchDirectQueryGlueCreateAccess
- AmazonOpenSearchIngestionFullAccess
- AmazonOpenSearchIngestionReadOnlyAccess
- AmazonOpenSearchIngestionServiceRolePolicy
- AmazonOpenSearchServerlessServiceRolePolicy
- AmazonOpenSearchServiceCognitoAccess
- AmazonOpenSearchServiceFullAccess
- AmazonOpenSearchServiceReadOnlyAccess
- AmazonOpenSearchServiceRolePolicy
- AmazonPersonalizeFullAccess
- AmazonPollyFullAccess
- AmazonPollyReadOnlyAccess
- AmazonPrometheusConsoleFullAccess
- AmazonPrometheusFullAccess
- AmazonPrometheusQueryAccess
- AmazonPrometheusRemoteWriteAccess
- AmazonPrometheusScraperServiceRolePolicy
- AmazonQFullAccess
- AmazonQLDBConsoleFullAccess
- AmazonQLDBFullAccess

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

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

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

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

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

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

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

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

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

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

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

- AWSDeepLensServiceRolePolicy
- AWSDeepRacerAccountAdminAccess
- AWSDeepRacerCloudFormationAccessPolicy
- AWSDeepRacerDefaultMultiUserAccess
- AWSDeepRacerFullAccess
- AWSDeepRacerRoboMakerAccessPolicy
- AWSDeepRacerServiceRolePolicy
- AWSDenyAll
- AWSDeviceFarmFullAccess
- AWSDeviceFarmServiceRolePolicy
- AWSDeviceFarmTestGridServiceRolePolicy
- AWSDirectConnectFullAccess
- AWSDirectConnectReadOnlyAccess
- AWSDirectConnectServiceRolePolicy
- AWSDirectoryServiceFullAccess
- AWSDirectoryServiceReadOnlyAccess
- AWSDiscoveryContinuousExportFirehosePolicy
- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSEC2VssSnapshotPolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS
- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy
- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy
- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2
- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy
- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy
- AWSElasticDisasterRecoveryFailbackPolicy
- AWSElasticDisasterRecoveryLaunchActionsPolicy
- AWSElasticDisasterRecoveryNetworkReplicationPolicy
- AWSElasticDisasterRecoveryReadOnlyAccess
- AWSElasticDisasterRecoveryRecoveryInstancePolicy
- AWSElasticDisasterRecoveryReplicationServerPolicy
- AWSElasticDisasterRecoveryServiceRolePolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy

- AWSElasticLoadBalancingServiceRolePolicy
- AWSElementalMediaConvertFullAccess
- AWSElementalMediaConvertReadOnly
- AWSElementalMediaLiveFullAccess
- AWSElementalMediaLiveReadOnly
- AWSElementalMediaPackageFullAccess
- AWSElementalMediaPackageReadOnly
- AWSElementalMediaPackageV2FullAccess
- AWSElementalMediaPackageV2ReadOnly
- AWSElementalMediaStoreFullAccess
- AWSElementalMediaStoreReadOnly
- AWSElementalMediaTailorFullAccess
- AWSElementalMediaTailorReadOnly
- AWSEnhancedClassicNetworkingMangementPolicy
- AWSEntityResolutionConsoleFullAccess
- AWSEntityResolutionConsoleReadOnlyAccess
- AWSFaultInjectionSimulatorEC2Access
- AWSFaultInjectionSimulatorECSAccess
- AWSFaultInjectionSimulatorEKSAccess
- AWSFaultInjectionSimulatorNetworkAccess
- AWSFaultInjectionSimulatorRDSAccess
- AWSFaultInjectionSimulatorSSMAccess
- AWSFinSpaceServiceRolePolicy
- AWSFMAdminFullAccess
- AWSFMAdminReadOnlyAccess
- AWSFMMemberReadOnlyAccess
- AWSForWordPressPluginPolicy
- AWSGitSyncServiceRolePolicy
- AWSGlobalAcceleratorSLRPolicy
- AWSGlueConsoleFullAccess

- AWSGlueConsoleSageMakerNotebookFullAccess
- AwsGlueDataBrewFullAccessPolicy
- AWSGlueDataBrewServiceRole
- AWSGlueSchemaRegistryFullAccess
- AWSGlueSchemaRegistryReadonlyAccess
- AWSGlueServiceNotebookRole
- AWSGlueServiceRole
- AwsGlueSessionUserRestrictedNotebookPolicy
- AwsGlueSessionUserRestrictedNotebookServiceRole
- AwsGlueSessionUserRestrictedPolicy
- AwsGlueSessionUserRestrictedServiceRole
- AWSGrafanaAccountAdministrator
- AWSGrafanaConsoleReadOnlyAccess
- AWSGrafanaWorkspacePermissionManagement
- AWSGrafanaWorkspacePermissionManagementV2
- AWSGreengrassFullAccess
- AWSGreengrassReadOnlyAccess
- AWSGreengrassResourceAccessRolePolicy
- AWSGroundStationAgentInstancePolicy
- AWSHealth_EventProcessorServiceRolePolicy
- AWSHealthFullAccess
- AWSHealthImagingFullAccess
- AWSHealthImagingReadOnlyAccess
- AWSIAMIdentityCenterAllowListForIdentityContext
- AWSIdentitySyncFullAccess
- AWSIdentitySyncReadOnlyAccess
- AWSImageBuilderFullAccess
- AWSImageBuilderReadOnlyAccess
- AWSImportExportFullAccess
- AWSImportExportReadOnlyAccess

- AWSIncidentManagerIncidentAccessServiceRolePolicy
- AWSIncidentManagerResolverAccess
- AWSIncidentManagerServiceRolePolicy
- AWSIoT1ClickFullAccess
- AWSIoT1ClickReadOnlyAccess
- AWSIoTAnalyticsFullAccess
- AWSIoTAnalyticsReadOnlyAccess
- AWSIoTConfigAccess
- AWSIoTConfigReadOnlyAccess
- AWSIoTDataAccess
- AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction
- AWSIoTDeviceDefenderAudit
- AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction
- AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction
- AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction
- AWSIoTDeviceDefenderUpdateCACertMitigationAction
- AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction
- AWSIoTDeviceTesterForFreeRTOSFullAccess
- AWSIoTDeviceTesterForGreengrassFullAccess
- AWSIoTEventsFullAccess
- AWSIoTEventsReadOnlyAccess
- AWSIoTFleetHubFederationAccess
- AWSIoTFleetwiseServiceRolePolicy
- AWSIoTFullAccess
- AWSIoTLogging
- AWSIoTOTAUpdate
- AWSIotRoboRunnerFullAccess
- AWSIotRoboRunnerReadOnly
- AWSIotRoboRunnerServiceRolePolicy
- AWSIoTRuleActions

- AWSIoTSiteWiseConsoleFullAccess
- AWSIoTSiteWiseFullAccess
- AWSIoTSiteWiseMonitorPortalAccess
- AWSIoTSiteWiseMonitorServiceRolePolicy
- AWSIoTSiteWiseReadOnlyAccess
- AWSIoTThingsRegistration
- AWSIoTTwinMakerServiceRolePolicy
- AWSIoTWirelessDataAccess
- AWSIoTWirelessFullAccess
- AWSIoTWirelessFullPublishAccess
- AWSIoTWirelessGatewayCertManager
- AWSIoTWirelessLogging
- AWSIoTWirelessReadOnlyAccess
- AWSIPAMServiceRolePolicy
- AWSIQContractServiceRolePolicy
- AWSIQFullAccess
- AWSIQPermissionServiceRolePolicy
- AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy
- AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy
- AWSKeyManagementServicePowerUser
- AWSLakeFormationCrossAccountManager
- AWSLakeFormationDataAdmin
- AWSLambda_FullAccess
- AWSLambda_ReadOnlyAccess
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB

- AWSLambdaKinesisExecutionRole
- AWSLambdaMSKExecutionRole
- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole
- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy
- AWSLicenseManagerMasterAccountRolePolicy
- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedServices_ContactsServiceRolePolicy
- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy
- AWSMarketplaceAmiIngestion
- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess
- AWSMarketplaceMeteringRegisterUsage
- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy

- AWSMarketplaceSellerFullAccess
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- AWSMediaConnectServicePolicy
- AWSMediaTailorServiceRolePolicy
- AWSMigrationHubDiscoveryAccess
- AWSMigrationHubDMSAccess
- AWSMigrationHubFullAccess
- AWSMigrationHubOrchestratorConsoleFullAccess
- AWSMigrationHubOrchestratorInstanceRolePolicy
- AWSMigrationHubOrchestratorPlugin
- AWSMigrationHubOrchestratorServiceRolePolicy
- AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess
- AWSMigrationHubRefactorSpaces-SSMAutomationPolicy
- AWSMigrationHubRefactorSpacesFullAccess
- AWSMigrationHubRefactorSpacesServiceRolePolicy
- AWSMigrationHubSMSAccess
- AWSMigrationHubStrategyCollector
- AWSMigrationHubStrategyConsoleFullAccess
- AWSMigrationHubStrategyServiceRolePolicy
- AWSMobileHub_FullAccess
- AWSMobileHub_ReadOnly
- AWSMSKReplicatorExecutionRole
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess
- AWSNetworkManagerServiceRolePolicy
- AWSOpsWorks_FullAccess
- AWSOpsWorksCloudWatchLogs

- AWSOpsWorksCMInstanceProfileRole
- AWSOpsWorksCMServiceRole
- AWSOpsWorksInstanceRegistration
- AWSOpsWorksRegisterCLI_EC2
- AWSOpsWorksRegisterCLI_OnPremises
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPriceListServiceFullAccess
- AWSPrivateCAAuditor
- AWSPrivateCAFullAccess
- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly
- AWSPrivateCAUser
- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy
- AWSProtonDeveloperAccess
- AWSProtonFullAccess

- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuickSightAssetBundleExportPolicy
- AWSQuickSightAssetBundleImportPolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess

- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess
- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy
- AWSServiceRoleForAmazonEKSNodegroup
- AWSServiceRoleForAmazonQDeveloper
- AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy
- AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy
- AWSServiceRoleForCodeGuru-Profiler
- AWSServiceRoleForCodeWhispererPolicy
- AWSServiceRoleForEC2ScheduledInstances
- AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy
- AWSServiceRoleForImageBuilder

- AWSServiceRoleForIoTSiteWise
- AWSServiceRoleForLogDeliveryPolicy
- AWSServiceRoleForMonitronPolicy
- AWSServiceRoleForNeptuneGraphPolicy
- AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWSServiceRoleForSMS
- AWSServiceRoleForUserSubscriptions
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting
- AWSShieldDRTAccessPolicy
- AWSShieldServiceRolePolicy
- AWSSSMForSAPServiceLinkedRolePolicy
- AWSSSMOpsInsightsServiceRolePolicy
- AWSSSODirectoryAdministrator
- AWSSSODirectoryReadOnly
- AWSSSOMasterAccountAdministrator
- AWSSSOMemberAccountAdministrator
- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess
- AWSStepFunctionsReadOnlyAccess
- AWSStorageGatewayFullAccess
- AWSStorageGatewayReadOnlyAccess
- AWSStorageGatewayServiceRolePolicy
- AWSSupplyChainFederationAdminAccess
- AWSSupportAccess
- AWSSupportAppFullAccess
- AWSSupportAppReadOnlyAccess
- AWSSupportPlansFullAccess

- AWSSupportPlansReadOnlyAccess
- AWSSupportServiceRolePolicy
- AWSSystemsManagerAccountDiscoveryServicePolicy
- AWSSystemsManagerChangeManagementServicePolicy
- AWSSystemsManagerForSAPFullAccess
- AWSSystemsManagerForSAPReadOnlyAccess
- AWSSystemsManagerOpsDataSyncServiceRolePolicy
- AWSThinkboxAssetServerPolicy
- AWSThinkboxAWSPortalAdminPolicy
- AWSThinkboxAWSPortalGatewayPolicy
- AWSThinkboxAWSPortalWorkerPolicy
- AWSThinkboxDeadlineResourceTrackerAccessPolicy
- AWSThinkboxDeadlineResourceTrackerAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginWorkerPolicy
- AWSTransferConsoleFullAccess
- AWSTransferFullAccess
- AWSTransferLoggingAccess
- AWSTransferReadOnlyAccess
- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy
- AWSTrustedAdvisorServiceRolePolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly
- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy

- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy
- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess
- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedDiscoveryServiceRolePolicy
- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess
- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- BatchServiceRolePolicy
- Billing
- CertificateManagerServiceRolePolicy
- ClientVPNServiceConnectionsRolePolicy
- ClientVPNServiceRolePolicy
- CloudFormationStackSetsOrgAdminServiceRolePolicy
- CloudFormationStackSetsOrgMemberServiceRolePolicy
- CloudFrontFullAccess
- CloudFrontReadOnlyAccess
- CloudHSMServiceRolePolicy
- CloudSearchFullAccess
- CloudSearchReadOnlyAccess
- CloudTrailServiceRolePolicy
- CloudWatch-CrossAccountAccess
- CloudWatchActionsEC2Access

- CloudWatchAgentAdminPolicy
- CloudWatchAgentServerPolicy
- CloudWatchApplicationInsightsFullAccess
- CloudWatchApplicationInsightsReadOnlyAccess
- CloudwatchApplicationInsightsServiceLinkedRolePolicy
- CloudWatchApplicationSignalsFullAccess
- CloudWatchApplicationSignalsReadOnlyAccess
- CloudWatchApplicationSignalsServiceRolePolicy
- CloudWatchAutomaticDashboardsAccess
- CloudWatchCrossAccountSharingConfiguration
- CloudWatchEventsBuiltInTargetExecutionAccess
- CloudWatchEventsFullAccess
- CloudWatchEventsInvocationAccess
- CloudWatchEventsReadOnlyAccess
- CloudWatchEventsServiceRolePolicy
- CloudWatchFullAccess
- CloudWatchFullAccessV2
- CloudWatchInternetMonitorServiceRolePolicy
- CloudWatchLambdaInsightsExecutionRolePolicy
- CloudWatchLogsCrossAccountSharingConfiguration
- CloudWatchLogsFullAccess
- CloudWatchLogsReadOnlyAccess
- CloudWatchNetworkMonitorServiceRolePolicy
- CloudWatchReadOnlyAccess
- CloudWatchSyntheticsFullAccess
- CloudWatchSyntheticsReadOnlyAccess
- ComprehendDataAccessRolePolicy
- ComprehendFullAccess
- ComprehendMedicalFullAccess
- ComprehendReadOnly

- ComputeOptimizerReadOnlyAccess
- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- EC2FastLaunchFullAccess
- EC2FastLaunchServiceRolePolicy
- EC2FleetTimeShiftableServiceRolePolicy
- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder
- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy
- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess
- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses
- ElementalActivationsReadOnlyAccess

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

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

- ROSAInstallerPolicy
- ROSAKMSProviderPolicy
- ROSAKubeControllerPolicy
- ROSAManageSubscription
- ROSANodePoolManagementPolicy
- ROSASRESupportPolicy
- ROSAWorkerInstancePolicy
- Route53RecoveryReadinessServiceRolePolicy
- Route53ResolverServiceRolePolicy
- S3StorageLensServiceRolePolicy
- SecretsManagerReadWrite
- SecurityAudit
- SecurityLakeServiceLinkedRole
- ServerMigration_ServiceRole
- ServerMigrationConnector
- ServerMigrationServiceConsoleFullAccess
- ServerMigrationServiceLaunchRole
- ServerMigrationServiceRoleForInstanceValidation
- ServiceQuotasFullAccess
- ServiceQuotasReadOnlyAccess
- ServiceQuotasServiceRolePolicy
- SimpleWorkflowFullAccess
- SplitCostAllocationDataServiceRolePolicy
- SupportUser
- SystemAdministrator
- TranslateFullAccess
- TranslateReadOnly
- ViewOnlyAccess
- VMImportExportRoleForAWSConnector
- VPCLatticeFullAccess

- VPCLatticeReadOnlyAccess
- VPCLatticeServicesInvokeAccess
- WAFLoggingServiceRolePolicy
- WAFRegionalLoggingServiceRolePolicy
- WAFV2LoggingServiceRolePolicy
- WellArchitectedConsoleFullAccess
- WellArchitectedConsoleReadOnlyAccess
- WorkLinkServiceRolePolicy

AccessAnalyzerServiceRolePolicy

Beschreibung: Erlauben Sie Access Analyzer, Ressourcenmetadaten zu analysieren

`AccessAnalyzerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Dezember 2019, 17:13 Uhr UTC
- Bearbeitete Zeit: 30. Mai 2024, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AdministratorAccess

Beschreibung: Bietet vollen Zugriff auf AWS Dienste und Ressourcen.

`AdministratorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AdministratorAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AdministratorAccess-Amplify

Beschreibung: Gewährt dem Konto Administratorrechte und ermöglicht gleichzeitig ausdrücklich den direkten Zugriff auf Ressourcen, die von Amplify-Anwendungen benötigt werden.

`AdministratorAccess-Amplify`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AdministratorAccess-Amplify` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 19:03 UTC
- Bearbeitete Zeit: 4. April 2024, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AdministratorAccess-AWSElasticBeanstalk

Beschreibung: Gewährt dem Konto Administratorrechte. Ermöglicht Entwicklern und Administratoren ausdrücklich den direkten Zugriff auf Ressourcen, die sie für die Verwaltung von AWS Elastic Beanstalk Beanstalk-Anwendungen benötigen

`AdministratorAccess-AWSElasticBeanstalk`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AdministratorAccess-AWSElasticBeanstalk` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. Januar 2021, 19:36 UTC
- Bearbeitete Zeit: 23. März 2023, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "codecommit:Get*",
        "codecommit:UploadArchive",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate*",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroup*",
        "ecs:CreateCluster",
        "ecs:DeRegisterTaskDefinition",
        "ecs:Describe*",
        "ecs:List*",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:Describe*",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "logs:Describe*",
```

```
        "rds:Describe*",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:*"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CancelUpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:SignalResource",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
```

```
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/Elastic-Beanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:TagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/awseb-e-*",
        "arn:aws:dynamodb:*:*:table/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*Rule",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetSecurityGroups"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
```

```
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/eb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/awseb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/eb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/eb-*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-elasticbeanstalk*",
        "arn:aws:iam::*:instance-profile/aws-elasticbeanstalk*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
      "Condition" : {
        "StringLike" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::aws:policy/AWSElasticBeanstalk*",
            "arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalk*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
```

```
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/autoscaling.amazonaws.com/
AWSServiceRoleForAutoScaling*",
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*",
        "arn:aws:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing*",
        "arn:aws:iam::*:role/aws-service-role/
managedupdates.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk*",
        "arn:aws:iam::*:role/aws-service-role/
maintenance.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "elasticbeanstalk.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "managedupdates.elasticbeanstalk.amazonaws.com",
            "maintenance.elasticbeanstalk.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
```

```
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*DBSubnetGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBInstance",
        "rds:DeleteDBSecurityGroup",
        "rds:ModifyDBInstance",
        "rds:RestoreDBInstanceFromDBSnapshot"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:secgrp:eb-*",
        "arn:aws:rds:*:*:snapshot:*",
        "arn:aws:rds:*:*:subgrp:awseb-e-*",
        "arn:aws:rds:*:*:subgrp:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:*QueueAttributes",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:SendMessage",
        "sqs:TagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessDeviceSetup

Beschreibung: Bieten Sie beim Geräte-Setup Zugriff auf AlexaForBusiness Dienste

`AlexaForBusinessDeviceSetup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AlexaForBusinessDeviceSetup` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:47 UTC
- Bearbeitete Zeit: 20. Mai 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessFullAccess

Beschreibung: Gewährt vollen Zugriff auf AlexaForBusiness Ressourcen und Zugriff auf verwandte AWS-Services

`AlexaForBusinessFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AlexaForBusinessFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:47 UTC
- Bearbeitete Zeit: 1. Juli 2020, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessGatewayExecution

Beschreibung: Stellen Sie Gateway-Ausführungszugriff auf AlexaForBusiness Dienste bereit

`AlexaForBusinessGatewayExecution`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AlexaForBusinessGatewayExecution` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:47 UTC
- Zeit bearbeitet: 30. November 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessLifesizeDelegatedAccessPolicy

Beschreibung: Ermöglichen Sie den Zugriff auf Lifesize AVS-Geräte

`AlexaForBusinessLifesizeDelegatedAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AlexaForBusinessLifesizeDelegatedAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Juni 2020, 19:46 UTC
- Bearbeitete Zeit: 12. Juni 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessNetworkProfileServicePolicy

Beschreibung: Diese Richtlinie ermöglicht es Alexa for Business, automatisierte Aufgaben auszuführen, die von Ihren Netzwerkprofilen geplant sind.

`AlexaForBusinessNetworkProfileServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. März 2019, 00:53 UTC
- Bearbeitete Zeit: 5. April 2019, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessPolyDelegatedAccessPolicy

Beschreibung: Ermöglichen Sie den Zugriff auf Poly AVS-Geräte

`AlexaForBusinessPolyDelegatedAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AlexaForBusinessPolyDelegatedAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. Oktober 2019, 19:48 UTC
- Bearbeitete Zeit: 16. Oktober 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessReadOnlyAccess

Beschreibung: Bieten Sie nur Lesezugriff auf AlexaForBusiness Dienste

`AlexaForBusinessReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AlexaForBusinessReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 30. November 2017, 16:47 UTC
- Zeit bearbeitet: 20. November 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAPIGatewayAdministrator

Beschreibung: Bietet vollen Zugriff auf das Erstellen/Bearbeiten/Löschen von APIs in Amazon API Gateway über die. AWS Management Console

`AmazonAPIGatewayAdministrator`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAPIGatewayAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:34 Uhr UTC
- Zeit bearbeitet: 9. Juli 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAPIGatewayInvokeFullAccess

Beschreibung: Bietet vollen Zugriff zum Aufrufen von APIs in Amazon API Gateway.

`AmazonAPIGatewayInvokeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAPIGatewayInvokeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:36 Uhr UTC
- Bearbeitete Zeit: 18. Dezember 2018, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAPIGatewayPushToCloudWatchLogs

Beschreibung: Ermöglicht API Gateway, Protokolle an das Benutzerkonto zu senden.

`AmazonAPIGatewayPushToCloudWatchLogs`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAPIGatewayPushToCloudWatchLogs` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. November 2015, 23:41 Uhr UTC

- Zeit bearbeitet: 11. November 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppFlowFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon AppFlow und Zugriff auf AWS Dienste, die als Flow-Quelle oder -Ziel (S3 und Redshift) unterstützt werden. Bietet auch Zugriff auf KMS zur Verschlüsselung

`AmazonAppFlowFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAppFlowFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juni 2020, 23:30 Uhr UTC
- Zeit bearbeitet: 28. Februar 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppFlowReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Appflow Flows

`AmazonAppFlowReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAppFlowReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juni 2020, 23:26 UTC
- Zeit bearbeitet: 28. Februar 2022, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppStreamFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon AppStream über die AWS Management Console.

`AmazonAppStreamFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAppStreamFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 28. August 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppStreamPCAAccess

Beschreibung: Amazon AppStream 2.0-Zugriff auf AWS Certificate Manager Private CA in Kundenkonten für zertifikatsbasierte Authentifizierung

`AmazonAppStreamPCAAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAppStreamPCAAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. Oktober 2022, 17:05 UTC
- Bearbeitete Zeit: 24. Oktober 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppStreamReadOnlyAccess

Beschreibung: Bietet Nur-Lesezugriff auf Amazon AppStream über die AWS Management Console.

`AmazonAppStreamReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAppStreamReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 7. Dezember 2016, 21:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppStreamServiceAccess

Beschreibung: Standardrichtlinie für die AppStream Amazon-Servicerolle.

`AmazonAppStreamServiceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAppStreamServiceAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. November 2016, 04:17 Uhr UTC
- Bearbeitete Zeit: 26. Juni 2020, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAthenaFullAccess

Beschreibung: Bieten Sie vollen Zugriff auf Amazon Athena und bereichsspezifischen Zugriff auf die Abhängigkeiten, die für das Abfragen, Schreiben von Ergebnissen und Datenmanagement erforderlich sind.

`AmazonAthenaFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAthenaFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 16:46 UTC
- Bearbeitete Zeit: 03. Januar 2024, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:StartColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseQueryResultsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
```

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

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAugmentedAIFullAccess

Beschreibung: Bietet Zugriff auf alle Operationen, die Amazon Augmented AI-Ressourcen ausführen können, einschließlich FlowDefinitions, HumanTaskUis und HumanLoops. Erlaubt keinen Zugriff zum Erstellen von FlowDefinitions Inhalten gegen das öffentliche Team.

`AmazonAugmentedAIFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAugmentedAIFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 16:21 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAugmentedAIHumanLoopFullAccess

Beschreibung: Ermöglicht den Zugriff auf die Ausführung aller Operationen an HumanLoops.

`AmazonAugmentedAIHumanLoopFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAugmentedAIHumanLoopFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 16:20 Uhr UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAugmentedAIIntegratedAPIAccess

Beschreibung: Bietet Zugriff auf alle Operationen, die Amazon Augmented AI-Ressourcen ausführen können, einschließlich FlowDefinitions, HumanTaskUis und HumanLoops. Bietet auch Zugriff auf die Operationen von Diensten, die in Amazon Augmented AI integriert sind.

`AmazonAugmentedAIIntegratedAPIAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonAugmentedAIIntegratedAPIAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. April 2020, 20:47 UTC
- Bearbeitete Zeit: 22. April 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Bedrock sowie eingeschränkten Zugriff auf verwandte Dienste, die von Amazon Bedrock benötigt werden

`AmazonBedrockFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonBedrockFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2023, 15:47 UTC
- Bearbeitete Zeit: 6. Dezember 2023, 15:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Bedrock

`AmazonBedrockReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonBedrockReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2023, 15:48 UTC
- Bearbeitete Zeit: 6. Dezember 2023, 15:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Sid" : "AmazonBedrockReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:ListFoundationModels",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:GetModelCustomizationJob",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListCustomModels",
        "bedrock:GetCustomModel",
        "bedrock:ListTagsForResource",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBraketFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Braket über das AWS Management Console und SDK. Bietet auch Zugriff auf verwandte Dienste (z. B. S3, Protokolle).

`AmazonBraketFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonBraketFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. August 2020, 20:12 Uhr UTC
- Bearbeitete Zeit: 19. April 2023, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:ListNotebookInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/amazon-
braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "braket:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/braket.amazonaws.com/
AWSServiceRoleForAmazonBraket*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "braket.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonBraketServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBraketJobsExecutionPolicy

Beschreibung: Gewährt Zugriff auf AWS-Services und Ressourcen, die für die Ausführung eines Amazon Braket-Jobs erforderlich sind, einschließlich S3, Cloudwatch, IAM und Braket

`AmazonBraketJobsExecutionPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonBraketJobsExecutionPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. November 2021, 19:34 UTC
- Bearbeitete Zeit: 28. November 2021, 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBraketServiceRolePolicy

Beschreibung: Ermöglicht Amazon Braket, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten

`AmazonBraketServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. August 2020, 17:12 Uhr UTC
- Zeit bearbeitet: 6. August 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeFullAccess

Beschreibung: Bietet vollen Zugriff auf die Amazon Chime Admin Console über die AWS Management Console.

`AmazonChimeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonChimeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. November 2017, 22:15 Uhr UTC
- Bearbeitete Zeit: 14. Dezember 2020, 21:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf die Amazon Chime Admin Console über die AWS Management Console.

`AmazonChimeReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonChimeReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. November 2017, 22:04 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeSDK

Beschreibung: Bietet Zugriff auf Amazon Chime SDK-Operationen

`AmazonChimeSDK`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonChimeSDK` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Februar 2020, 21:53 UTC
- Bearbeitete Zeit: 10. Januar 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Beschreibung: Verwaltete Richtlinie für die verknüpfte Rolle mit dem Amazon Chime SDK MediaPipelines Service

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. April 2022, 22:02 UTC
- Bearbeitete Zeit: 8. Dezember 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeSDKMessagingServiceRolePolicy

Beschreibung: Ermöglicht Amazon Chime SDK Messaging den Zugriff auf AWS Ressourcen und die Aktivierung der Messaging-Funktionalität

`AmazonChimeSDKMessagingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 03. März 2023, 01:43 UTC
- Bearbeitete Zeit: 03. März 2023, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Ressourcen, die von Amazon Chime verwendet oder verwaltet werden

`AmazonChimeServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. September 2019, 22:25 Uhr UTC
- Bearbeitete Zeit: 30. September 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeTranscriptionServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Chime, in Ihrem Namen auf Amazon Transcribe und Amazon Transcribe Medical zuzugreifen

`AmazonChimeTranscriptionServiceLinkedRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. August 2021, 21:47 UTC
- Bearbeitete Zeit: 4. August 2021, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeUserManagement

Beschreibung: Bietet Benutzerverwaltungszugriff auf die Amazon Chime Admin Console über die AWS Management Console.

`AmazonChimeUserManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonChimeUserManagement` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. November 2017, 22:17 UTC
- Bearbeitete Zeit: 18. Februar 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Beschreibung: Verwaltete Richtlinie für Service Linked Role für Amazon Chime VoiceConnector

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. September 2019, 22:16 Uhr UTC
- Bearbeitete Zeit: 14. April 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudDirectoryFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Cloud Directory Service.

`AmazonCloudDirectoryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCloudDirectoryFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Februar 2017, 00:41 UTC
- Zeit bearbeitet: 25. Februar 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudDirectoryReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Cloud Directory Service.

`AmazonCloudDirectoryReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCloudDirectoryReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Februar 2017, 23:42 UTC
- Zeit bearbeitet: 28. Februar 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchEvidentlyFullAccess

Beschreibung: Bietet nur vollen Zugriff auf Amazon CloudWatch Eviently. Bietet auch Zugriff auf verwandte Amazon S3, Amazon SNS CloudWatch, Amazon und andere verwandte Dienste.

`AmazonCloudWatchEvidentlyFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCloudWatchEvidentlyFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 15:10 Uhr UTC
- Bearbeitete Zeit: 29. November 2021, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchEvidentlyReadOnlyAccess

Beschreibung: Bietet CloudWatch offensichtlich nur Lesezugriff auf Amazon

`AmazonCloudWatchEvidentlyReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCloudWatchEvidentlyReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 15:08 UTC
- Bearbeitete Zeit: 29. November 2021, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchEvidentlyServiceRolePolicy

Beschreibung: Ermöglicht CloudWatch Evidently Service, die zugehörigen AWS Ressourcen im Namen des Kunden zu verwalten

`AmazonCloudWatchEvidentlyServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. September 2022, 17:25 UTC
- Bearbeitete Zeit: 13. September 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchRUMFullAccess

Beschreibung: Gewährt volle Zugriffsberechtigungen für den Amazon CloudWatch RUM-Service

`AmazonCloudWatchRUMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCloudWatchRUMFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 15:46 Uhr UTC
- Bearbeitete Zeit: 29. November 2021, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchRUMReadOnlyAccess

Beschreibung: Gewährt Nur-Lese-Berechtigungen für den Amazon CloudWatch RUM-Service

`AmazonCloudWatchRUMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCloudWatchRUMReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 15:43 Uhr UTC

- Zeit bearbeitet: 28. Oktober 2022, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchRUMServiceRolePolicy

Beschreibung: Erteilt Amazon CloudWatch RUM Service die Erlaubnis, Überwachungsdaten für andere relevante AWS Dienste zu veröffentlichen

`AmazonCloudWatchRUMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. November 2021, 23:17 UTC
- Bearbeitete Zeit: 22. Februar 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeCatalystFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon CodeCatalyst

`AmazonCodeCatalystFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeCatalystFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 20. April 2023, 16:50 UTC
- Bearbeitete Zeit: 20. April 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeCatalystReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon CodeCatalyst

`AmazonCodeCatalystReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeCatalystReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. April 2023, 16:49 UTC
- Bearbeitete Zeit: 20. April 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeCatalystSupportAccess

Beschreibung: Ermöglicht Amazon, AWS Support Fälle in Ihrem Namen CodeCatalyst zu erstellen, zu aktualisieren und zu lösen.

`AmazonCodeCatalystSupportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeCatalystSupportAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 12:34 UTC
- Bearbeitete Zeit: 20. April 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruProfilerAgentAccess

Beschreibung: Bietet Zugriff, der für den Amazon CodeGuru Profiler-Agent erforderlich ist.

`AmazonCodeGuruProfilerAgentAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeGuruProfilerAgentAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Februar 2021, 22:11 UTC
- Bearbeitete Zeit: 5. Mai 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruProfilerFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeGuruProfilerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 10:13 Uhr UTC
- Bearbeitete Zeit: 15. Juli 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruProfilerReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeGuruProfilerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 10:30 Uhr UTC
- Bearbeitete Zeit: 27. Juni 2020, 23:52 UTC

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

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruReviewerFullAccess

Beschreibung: Gewährt vollen Zugriff auf Amazon CodeGuru Reviewer und bereichsspezifischen Zugriff auf erforderliche Abhängigkeiten.

`AmazonCodeGuruReviewerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeGuruReviewerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 08:33 UTC
- Bearbeitete Zeit: 29. August 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruReviewerReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon CodeGuru Reviewer.

`AmazonCodeGuruReviewerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeGuruReviewerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 08:48 UTC
- Bearbeitete Zeit: 29. August 2020, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruReviewerServiceRolePolicy

Beschreibung: Eine servicebezogene Rolle, die Amazon CodeGuru Reviewer benötigt, um in Ihrem Namen auf Ressourcen zuzugreifen.

`AmazonCodeGuruReviewerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Dezember 2019, 05:31 Uhr UTC
- Bearbeitete Zeit: 27. November 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruSecurityFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon CodeGuru Security.

`AmazonCodeGuruSecurityFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeGuruSecurityFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Mai 2023, 21:03 UTC
- Bearbeitete Zeit: 9. Mai 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruSecurityScanAccess

Beschreibung: Bietet Zugriff, der für die Arbeit mit Amazon CodeGuru Security-Scans erforderlich ist.

`AmazonCodeGuruSecurityScanAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCodeGuruSecurityScanAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Mai 2023, 20:54 UTC
- Bearbeitete Zeit: 9. Mai 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoDeveloperAuthenticatedIdentities

Beschreibung: Bietet Zugriff auf Amazon Cognito Cognito-APIs, um von Entwicklern authentifizierte Identitäten von Ihrem Authentifizierungs-Backend aus zu unterstützen.

`AmazonCognitoDeveloperAuthenticatedIdentities`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCognitoDeveloperAuthenticatedIdentities` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. März 2015, 17:22 Uhr UTC
- Bearbeitete Zeit: 24. März 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoIdpEmailServiceRolePolicy

Beschreibung: Ermöglicht dem Amazon Cognito User Pools-Service, Ihre SES-Identitäten für den E-Mail-Versand zu verwenden

`AmazonCognitoIdpEmailServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. März 2019, 21:32 Uhr UTC
- Bearbeitete Zeit: 21. März 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoIdpServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon Cognito Cognito-Benutzerpools verwendet oder verwaltet werden

`AmazonCognitoIdpServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. Juni 2020, 22:30 Uhr UTC
- Bearbeitete Zeit: 26. Juni 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoPowerUser

Beschreibung: Bietet administrativen Zugriff auf bestehende Amazon Cognito Cognito-Ressourcen. Sie benötigen AWS-Konto Administratorrechte, um neue Cognito-Ressourcen zu erstellen.

`AmazonCognitoPowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCognitoPowerUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. März 2015, 17:14 Uhr UTC
- Bearbeitete Zeit: 1. Juni 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "iam:ListRoles",
```

```
        "iam:ListOpenIdConnectProviders",
        "iam:GetRole",
        "iam:ListSAMLProviders",
        "iam:GetSAMLProvider",
        "kinesis:ListStreams",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "sns:GetSMSSandboxAccountStatus",
        "sns:ListPlatformApplications",
        "ses:ListIdentities",
        "ses:GetIdentityVerificationAttributes",
        "mobiletargeting:GetApps",
        "acm:ListCertificates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "cognito-idp.amazonaws.com",
            "email.cognito-idp.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdp*",
        "arn:aws:iam::*:role/aws-service-role/email.cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdpEmail*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoReadOnly

Beschreibung: Bietet Lesezugriff auf Amazon Cognito Cognito-Ressourcen.

`AmazonCognitoReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCognitoReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. März 2015, 17:06 UTC
- Bearbeitete Zeit: 1. August 2019, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Beschreibung: Diese Richtlinie definiert die Berechtigungen, die für nicht authentifizierte Identitäten für Cognito-Identitätspools zulässig sind. Diese Richtlinie ist nicht dafür vorgesehen, als eigenständige Berechtigungsrichtlinie verwendet zu werden. Sie dient als Schutzmaßnahme gegen übermäßig freizügige Richtlinien für Rollen in einem Identitätspool. Fügen Sie diese Richtlinie keiner Rolle hinzu, da Cognito Identity Service sie bei der Erstellung von Anmeldeinformationen automatisch als Richtlinie mit eingeschränktem Geltungsbereich einbezieht. Die Rechte für den temporären Zugriff auf andere AWS Ressourcen über den erweiterten Ablauf werden nun durch die Schnittmenge zwischen der Rolle, die mit der Identität des nicht authentifizierten Benutzers verknüpft ist, die von einem Dienst bereitgestellt wird, und den Rechten definiert, die in dieser verwalteten Richtlinie, die Cognito gehört, gewährt werden.

`AmazonCognitoUnAuthedIdentitiesSessionPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCognitoUnAuthedIdentitiesSessionPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Juli 2023, 23:04 UTC
- Bearbeitete Zeit: 19. Juli 2023, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoUnauthenticatedIdentities

Beschreibung: Diese Richtlinie definiert die Berechtigungen, die für nicht authentifizierte Identitäten für Cognito-Identitätspools zulässig sind. Dies muss nicht an Ihre Unauth-Rolle angehängt werden, da Cognito Identity Service es bei der Erstellung von Anmeldeinformationen automatisch als eingeschränkte Richtlinie einbezieht. Die Rechte für den temporären Zugriff auf andere AWS Ressourcen über den erweiterten Ablauf werden nun durch die Schnittmenge zwischen der Rolle, die

mit der Identität des nicht authentifizierten Benutzers verknüpft ist, die von einem Dienst bereitgestellt wird, und den Rechten definiert, die in dieser verwalteten Richtlinie, die Cognito gehört, gewährt werden.

`AmazonCognitoUnauthenticatedIdentities`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonCognitoUnauthenticatedIdentities` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Februar 2023, 22:36 UTC
- Bearbeitete Zeit: 1. Februar 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnect_FullAccess

Beschreibung: Der Zweck dieser Richtlinie besteht darin, AWS Connect-Benutzern Berechtigungen zu gewähren, die für die Verwendung von Connect-Ressourcen erforderlich sind. Diese Richtlinie bietet vollen Zugriff auf AWS Connect-Ressourcen über die Connect Console und öffentliche APIs.

`AmazonConnect_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonConnect_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2020, 19:54 UTC
- Bearbeitete Zeit: 7. März 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectCampaignsServiceLinkedRolePolicy

Beschreibung: Richtlinie für die mit dem Dienst Amazon Connect Campaigns verknüpfte Rolle

`AmazonConnectCampaignsServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. September 2021, 20:54 UTC
- Bearbeitete Zeit: 8. November 2023, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "connect:StopContact"
      ],
      "Resource" : "arn:aws:connect:*:*:instance/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectReadOnlyAccess

Beschreibung: Erteilt die Berechtigung zum Anzeigen der Amazon Connect Connect-Instances in Ihrem AWS-Konto.

`AmazonConnectReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonConnectReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Oktober 2018, 21:00 Uhr UTC
- Bearbeitete Zeit: 6. November 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Connect, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

`AmazonConnectServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. September 2018, 00:21 UTC
- Bearbeitete Zeit: 24. Mai 2024, 01:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v16 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

```
    },
    {
      "Sid" : "AllowListLexBotAccess",
      "Effect" : "Allow",
      "Action" : [
        "lex:ListBots",
        "lex:ListBotAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:SearchProfiles",
        "profile:CreateProfile",
        "profile:UpdateProfile",
        "profile:AddProfileKey",
        "profile:ListProfileObjectTypes",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListCalculatedAttributesForProfile",
        "profile:GetDomain",
        "profile:ListIntegrations"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfileObjects",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjects",
        "profile:GetProfileObjectType"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowListIntegrationForCustomerProfile",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListAccountIntegrations"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowReadForCustomerProfileObjectTemplates",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjectTypeTemplates",
        "profile:GetProfileObjectTypeTemplate"
      ],
      "Resource" : "arn:aws:profile:*:*:/templates*"
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:CreateContent",
        "wisdom:DeleteContent",
        "wisdom:CreateKnowledgeBase",
        "wisdom:GetAssistant",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetContent",
        "wisdom:GetRecommendations",
        "wisdom:GetSession",
        "wisdom:NotifyRecommendationsReceived",
        "wisdom:QueryAssistant",
        "wisdom:StartContentUpload",
        "wisdom:UpdateContent",
        "wisdom:UntagResource",
        "wisdom:TagResource",
        "wisdom:CreateSession",
        "wisdom:CreateQuickResponse",
        "wisdom:GetQuickResponse",
        "wisdom:SearchQuickResponses",
        "wisdom:StartImportJob",
        "wisdom:GetImportJob",
        "wisdom:ListImportJobs",
        "wisdom:ListQuickResponses",
        "wisdom:UpdateQuickResponse",
        "wisdom:DeleteQuickResponse",
        "wisdom:PutFeedback",
        "wisdom:ListContentAssociations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetCalculatedAttributeForProfile",
        "profile:CreateCalculatedAttributeDefinition",
        "profile:DeleteCalculatedAttributeDefinition",
        "profile:GetCalculatedAttributeDefinition",
        "profile:UpdateCalculatedAttributeDefinition"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/calculated-attributes/*"
      ]
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
```

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectSynchronizationServiceRolePolicy

Beschreibung: Ermöglicht Amazon Connect, AWS Ressourcen in Ihrem Namen regionsübergreifend zu synchronisieren.

`AmazonConnectSynchronizationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. Oktober 2023, 22:38 UTC
- Bearbeitete Zeit: 27. Oktober 2023, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "connect:CreateUser*",
        "connect:UpdateUser*",
        "connect:DeleteUser*",
        "connect:DescribeUser*",
        "connect:ListUser*",
        "connect:CreateRoutingProfile",
        "connect:UpdateRoutingProfile*",
        "connect:DeleteRoutingProfile",
        "connect:DescribeRoutingProfile",
        "connect:ListRoutingProfile*",
        "connect:CreateAgentStatus",
        "connect:UpdateAgentStatus",
        "connect:DescribeAgentStatus",
        "connect:ListAgentStatuses",
        "connect:CreateQuickConnect",
        "connect:UpdateQuickConnect*",
        "connect:DeleteQuickConnect",
        "connect:DescribeQuickConnect",
        "connect:ListQuickConnects",
        "connect:CreateHoursOfOperation",
        "connect:UpdateHoursOfOperation",
        "connect:DeleteHoursOfOperation",
        "connect:DescribeHoursOfOperation",
        "connect:ListHoursOfOperations",
        "connect:CreateQueue",
        "connect:UpdateQueue*",
        "connect:DeleteQueue",
        "connect:DescribeQueue",
        "connect:ListQueue*",
        "connect:CreatePrompt",
        "connect:UpdatePrompt",
        "connect:DeletePrompt",
        "connect:DescribePrompt",
        "connect:ListPrompts",
        "connect:GetPromptFile",
        "connect:CreateSecurityProfile",
        "connect:UpdateSecurityProfile",
        "connect:DeleteSecurityProfile",
        "connect:DescribeSecurityProfile",
        "connect:ListSecurityProfile*",
        "connect:CreateContactFlow*",
        "connect:UpdateContactFlow*",
        "connect:DeleteContactFlow*",
        "connect:DescribeContactFlow*",
```

```
        "connect:ListContactFlow*",
        "connect:BatchGetFlowAssociation",
        "connect:CreatePredefinedAttribute",
        "connect:UpdatePredefinedAttribute",
        "connect:DeletePredefinedAttribute",
        "connect:DescribePredefinedAttribute",
        "connect:ListPredefinedAttributes",
        "connect:ListTagsForResource",
        "connect:TagResource",
        "connect:UntagResource",
        "connect:ListTrafficDistributionGroups",
        "connect:ListPhoneNumbersV2",
        "connect:UpdatePhoneNumber",
        "connect:DescribePhoneNumber",
        "connect:Associate*",
        "connect:Disassociate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectVoiceIDFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Connect Voice ID

`AmazonConnectVoiceIDFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonConnectVoiceIDFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. September 2021, 19:04 UTC
- Bearbeitete Zeit: 26. September 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneDomainExecutionRolePolicy

Beschreibung: Standardrichtlinie für die DataZone DomainExecutionRole Servicerolle von Amazon. Diese Rolle wird von Amazon verwendet, DataZone um Daten in der DataZone Amazon-Domain zu katalogisieren, zu entdecken, zu verwalten, zu teilen und zu analysieren.

`AmazonDataZoneDomainExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneDomainExecutionRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. September 2023, 21:55 UTC
- Bearbeitete Zeit: 1. April 2024, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneEnvironmentRolePermissionsBoundary

Beschreibung: Amazon DataZone erstellt IAM-Rollen für Umgebungen, um Datenanalyseaktionen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

`AmazonDataZoneEnvironmentRolePermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneEnvironmentRolePermissionsBoundary` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. September 2023, 23:38 UTC
- Bearbeitete Zeit: 17. November 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DataZone über die AWS Management Console sowie eingeschränkten Zugriff auf verwandte Dienste, die von Amazon benötigt werden.

`AmazonDataZoneFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2023, 20:06 UTC
- Bearbeitete Zeit: 23. April 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

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

```
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd_*"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneFullUserAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DataZone, ermöglicht jedoch nicht die Verwaltung von Domains, Benutzern oder zugehörigen Konten.

`AmazonDataZoneFullUserAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneFullUserAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2023, 21:06 UTC
- Bearbeitete Zeit: 1. April 2024, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:PostTimeSeriesDataPoints",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
```

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneGlueManageAccessRolePolicy

Beschreibung: Die Richtlinie gewährt Amazon Berechtigungen, die es Amazon DataZone ermöglichen, Veröffentlichungen und Zugriffsberechtigungen für Daten zu aktivieren.

`AmazonDataZoneGlueManageAccessRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneGlueManageAccessRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. September 2023, 20:21 UTC
- Bearbeitete Zeit: 03. Juni 2024, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Sid" : "GlueTagDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "glue:GetTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLikeIfExists" : {
          "aws:TagKeys" : "DataZoneDiscoverable_*"
        }
      }
    },
    {
      "Sid" : "GlueDataQualityPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListDataQualityResults",
        "glue:GetDataQualityResult"
      ],
      "Resource" : "arn:aws:glue:*:*:dataQualityRuleset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTableDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
```

```
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:GrantPermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares",
```

```
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSDecryptPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/datazone:projectId" : "proj-all"
        }
```

```
      }
    },
    {
      "Sid" : "GetRoleForDataZone",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
      ]
    },
    {
      "Sid" : "PassRoleForDataLocationRegistration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZonePortalFullAccessPolicy

Beschreibung: Bietet vollen Zugriff auf DataZone Amazon-APIs

`AmazonDataZonePortalFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZonePortalFullAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. März 2023, 18:24 UTC
- Bearbeitete Zeit: 26. März 2023, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZonePreviewConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Vorschauversion von Amazon DataZone über die AWS Management Console. Bietet auch ausgewählten Zugriff auf andere verwandte Dienste.

`AmazonDataZonePreviewConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZonePreviewConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. März 2023, 15:16 UTC
- Bearbeitete Zeit: 13. Juli 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneProjectDeploymentPermissionsBoundary

Beschreibung: Amazon DataZone erstellt IAM-Rollen, die es für die Bereitstellung von Datenanalyseprojekten verwendet. DataZone verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

`AmazonDataZoneProjectDeploymentPermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneProjectDeploymentPermissionsBoundary` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. März 2023, 02:54 UTC
- Bearbeitete Zeit: 4. April 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneProjectRolePermissionsBoundary

Beschreibung: Amazon DataZone erstellt IAM-Rollen für Projekte, um Datenanalyseaktionen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

`AmazonDataZoneProjectRolePermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneProjectRolePermissionsBoundary` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. März 2023, 02:51 UTC
- Bearbeitete Zeit: 21. März 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneRedshiftGlueProvisioningPolicy

Beschreibung: Amazon DataZone ist ein Datenverwaltungsservice, mit dem Sie Ihre Daten katalogisieren, ermitteln, verwalten, teilen und analysieren können. Mit Amazon DataZone können Sie Ihre Daten über Konten und unterstützte Regionen hinweg teilen und darauf zugreifen. Amazon DataZone vereinfacht Ihre Erfahrung mit allen AWS Services, einschließlich, aber nicht beschränkt auf Amazon Redshift, Amazon Athena, AWS Glue und AWS Lake Formation.

`AmazonDataZoneRedshiftGlueProvisioningPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneRedshiftGlueProvisioningPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2023, 20:19 UTC
- Bearbeitete Zeit: 12. März 2024, 16:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "athena:GetWorkGroup",
        "logs:DescribeLogGroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift:DescribeClusters",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
```

```
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:TagLogGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupCreation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupManagement",
```

```
      "Action" : [
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:GetPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentS3ValidationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSDecryptPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "RedshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ListSchemas",
        "redshift-data:ExecuteStatement"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "DescribeStatementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSecretValuePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneRedshiftManageAccessRolePolicy

Beschreibung: Diese Richtlinie erteilt Amazon die DataZone Erlaubnis, Amazon Redshift Redshift-Daten im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf veröffentlichte Amazon Redshift- oder Amazon Redshift Serverless-Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

`AmazonDataZoneRedshiftManageAccessRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneRedshiftManageAccessRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. September 2023, 20:15 UTC
- Bearbeitete Zeit: 16. November 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Sid" : "redshiftDataScopeDownPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "listSecretsPermission",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "getWorkgroupPermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetWorkgroup",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "getNamespacePermission",
      "Effect" : "Allow",
```

```
      "Action" : "redshift-serverless:GetNamespace",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "redshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "dataSharesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "associateDataShareConsumerPermission",
      "Effect" : "Allow",
      "Action" : "redshift:AssociateDataShareConsumer",
      "Resource" : "arn:aws:redshift:*:*:datashare:*/datazone*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Beschreibung: Die AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary Richtlinie ist die Liste der Berechtigungen, die für eine Ausführungsrolle zulässig sind, die in einer von Amazon DataZone bereitgestellten SageMaker Umgebung erstellt wurde.

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2024, 23:01 UTC
- Bearbeitete Zeit: 8. Mai 2024, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowSageMakerProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile",
        "sagemaker:UpdateUserProfile",
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:*/*"
    },
    {
      "Sid" : "AllowLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowAddTagsForAppAndSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateApp",
            "CreateSpace"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListSpaces",
        "sagemaker:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
```

```
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
```

```
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
```

```
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*",
        "datazone:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "groundtruthlabeling:*",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
```

```
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowRAMInvitation",
      "Effect" : "Allow",
      "Action" : "ram:AcceptResourceShareInvitation",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "dzd_*"
        }
      }
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker*",
        "arn:aws:ecr:*:*:repository/datazone*"
      ]
    },
    {
```

```
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
```

```
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "states.amazonaws.com",
```

```
            "lakeformation.amazonaws.com",
            "events.amazonaws.com",
            "sagemaker.amazonaws.com",
            "forecast.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:domain/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
```

```
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:ListJobs",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:GetTable",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:ListSchemas",
        "glue:BatchGetJobs",
        "glue:GetConnection",
```

```
        "glue:GetDatabase"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueActionsWithEnvironmentTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:ListSchemas",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
```

```
        "glue:CreateWorkflow",
        "glue:*DataQuality*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGlueDefaultAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:RunStatement"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:connection/dz-sm-*",
        "arn:aws:glue:*:*:session/*"
      ]
    },
    {
      "Sid" : "AllowRedshiftClusterActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowCreateClusterUser",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterUser"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*"
      ]
    },
    {
      "Sid" : "AllowCreateSecretActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd_*",
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd_*"
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
```

```
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventBridgeRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEMR",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowSSOAction",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyNotAction",
      "Effect" : "Deny",
      "NotAction" : [
        "sagemaker:*",
        "sagemaker-geospatial:*",
        "sqlworkbench:*",
        "datazone:*",
        "forecast:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
```

```
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:StartImageScan",
        "ecr:TagResource",
        "ecr:UntagResource",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource",
        "fsx:DescribeFileSystems",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
```

```
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGet*",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:Get*",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:List*",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreateDatabase",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
```

```
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "groundtruthlabeling:*",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant",
        "lakeformation:GetDataAccess",
        "lambda:ListFunctions",
        "lambda:InvokeFunction",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "ram:AcceptResourceShareInvitation",
        "rds:DescribeDBInstances",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
```

```
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors",
        "s3:DeleteObjectVersion",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:TagResource",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
```

```
        "states:StopExecution",
        "states:UpdateStateMachine",
        "tag:GetResources",
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneSageMakerManageAccessRolePolicy

Beschreibung: Die AmazonDataZoneSageMakerManageAccessRolePolicy Richtlinie gewährt Amazon DataZone die erforderlichen Berechtigungen, um Benutzern Zugriff auf verschiedene Ressourcen in der SageMaker Umgebung zu gewähren.

`AmazonDataZoneSageMakerManageAccessRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneSageMakerManageAccessRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2024, 23:34 UTC
- Bearbeitete Zeit: 23. April 2024, 23:34 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:ListTags",
        "sagemaker:DescribeDomain",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelPackageGroupPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:DeleteModelPackageGroupPolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerRAMResourcePolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutResourcePolicy",
        "sagemaker:GetResourcePolicy",
        "sagemaker:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:feature-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMTagResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ram:TagResource"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMDeleteResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMCreateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "sagemaker:*"
          ]
        },
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerS3BucketPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:DeleteRepositoryPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSReadPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSGrantPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneSageMakerProvisioningRolePolicy

Beschreibung: Die AmazonDataZoneSageMakerProvisioningRolePolicy Richtlinie gewährt Amazon DataZone die für die Zusammenarbeit mit Amazon SageMaker erforderlichen Berechtigungen.

`AmazonDataZoneSageMakerProvisioningRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDataZoneSageMakerProvisioningRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2024, 23:32 UTC
- Bearbeitete Zeit: 23. April 2024, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Sid" : "CreateSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false",
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
```

```
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ],
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "sagemaker:ListDomains"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSKeyValidation",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGluePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:CreateConnection",
        "glue:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveFullAccess

Beschreibung: Bietet vollen Zugriff auf den Amazon Detective Service und bereichsspezifischen Zugriff auf die Abhängigkeiten der Konsolen-Benutzeroberfläche

`AmazonDetectiveFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDetectiveFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. April 2020, 17:57 UTC
- Bearbeitete Zeit: 17. Mai 2023, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveInvestigatorAccess

Beschreibung: Bietet Ermittlern Zugriff auf den Amazon Detective Service und bereichsspezifischen Zugriff auf die Benutzeroberflächenabhängigkeiten der Konsole. Diese Richtlinie gewährt die Erlaubnis, Detective zu Ermittlungszwecken zu nutzen, und gewährt eingeschränkten Schreibzugriff auf Guardduty.

`AmazonDetectiveInvestigatorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDetectiveInvestigatorAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Januar 2023, 15:24 UTC
- Bearbeitete Zeit: 27. November 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveMemberAccess

Beschreibung: Bietet Mitgliedern Zugriff auf den Amazon Detective Service und bereichsspezifischen Zugriff auf die Abhängigkeiten der Konsolen-Benutzeroberfläche.

`AmazonDetectiveMemberAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDetectiveMemberAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Januar 2023, 15:16 UTC
- Bearbeitete Zeit: 17. Januar 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveOrganizationsAccess

Beschreibung: Bietet Organizations Zugriff auf die Verwaltung des delegierten Administrators für Amazon Detective und bereichsspezifischen Zugriff auf die Benutzeroberflächenabhängigkeiten der Konsole. Dadurch wird auch die Erlaubnis erteilt, eine dienstbezogene Rolle für Detective zu erstellen.

`AmazonDetectiveOrganizationsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDetectiveOrganizationsAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. März 2023, 15:20 UTC
- Bearbeitete Zeit: 2. März 2023, 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Detective, Serviceanrufe in Ihrem Namen zu tätigen

`AmazonDetectiveServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2021, 19:47 UTC
- Bearbeitete Zeit: 18. November 2021, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruConsoleFullAccess

Beschreibung: Die Richtlinie gewährt vollen Zugriff auf die DevOps Guru-Konsole.

`AmazonDevOpsGuruConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDevOpsGuruConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Dezember 2021, 18:43 UTC

- Bearbeitete Zeit: 25. August 2022, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DevOps Guru.

`AmazonDevOpsGuruFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDevOpsGuruFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 16:38 UTC
- Zeit bearbeitet: 25. August 2022, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruOrganizationsAccess

Beschreibung: Stellen Sie Zugriff bereit, um Amazon DevOps Guru innerhalb einer Organisation zu aktivieren und zu verwalten.

`AmazonDevOpsGuruOrganizationsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDevOpsGuruOrganizationsAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2021, 23:50 UTC
- Bearbeitete Zeit: 15. November 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf die Amazon DevOps Guru Console.

`AmazonDevOpsGuruReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDevOpsGuruReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 16:34 UTC
- Zeit bearbeitet: 25. August 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruServiceRolePolicy

Beschreibung: Eine servicebezogene Rolle, die Amazon benötigt, DevOpsGuru um auf Ihre Ressourcen zugreifen zu können.

`AmazonDevOpsGuruServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Dezember 2020, 10:24 Uhr UTC
- Bearbeitete Zeit: 10. Januar 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDMSCloudWatchLogsRole

Beschreibung: Ermöglicht den Zugriff auf das Hochladen von DMS-Replikationsprotokollen in Cloudwatch-Protokolle im Kundenkonto.

`AmazonDMSCloudWatchLogsRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDMSCloudWatchLogsRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. Januar 2016, 23:44 UTC
- Bearbeitete Zeit: 23. Mai 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDMSRedshiftS3Role

Beschreibung: Ermöglicht den Zugriff auf die Verwaltung von S3-Einstellungen für Redshift-Endpunkte für DMS.

`AmazonDMSRedshiftS3Role`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDMSRedshiftS3Role` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 20. April 2016, 17:05 UTC
- Bearbeitete Zeit: 8. Juli 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDMSVPCManagementRole

Beschreibung: Bietet Zugriff auf die Verwaltung von VPC-Einstellungen für AWS verwaltete Kundenkonfigurationen

`AmazonDMSVPCManagementRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDMSVPCManagementRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 18. November 2015, 16:33 UTC
- Bearbeitete Zeit: 23. Mai 2016, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDB-ElasticServiceRolePolicy

Beschreibung: Ermöglicht Amazon DocumentDB-Elastic, AWS Ressourcen in Ihrem Namen zu verwalten.

`AmazonDocDB-ElasticServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2022, 14:17 UTC
- Zeit bearbeitet: 30. November 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung von Amazon DocumentDB mit MongoDB-Kompatibilität mithilfe von. AWS Management Console Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos, Berechtigungen zum Erstellen und Bearbeiten von Amazon EC2 EC2-Instances und VPC-Konfigurationen, Berechtigungen zum Anzeigen und Auflisten von Schlüsseln in Amazon KMS sowie vollen Zugriff auf Amazon RDS und Amazon Neptune gewährt.

`AmazonDocDBConsoleFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDocDBConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Januar 2019, 20:37 UTC
- Bearbeitete Zeit: 30. November 2022, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
```

```
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
```

```
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
```

```
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBElasticFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DocumentDB Elastic Clusters und andere erforderliche Berechtigungen für dessen Abhängigkeiten, einschließlich EC2 SecretsManager, KMS CloudWatch und IAM.

`AmazonDocDBElasticFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDocDBElasticFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 5. Juni 2023, 13:51 UTC
- Bearbeitete Zeit: 21. Juni 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ],
          "aws:ResourceTag/DocDBElasticFullAccess" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/DocDBElasticFullAccess" : "*",
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBElasticReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon DoCDB-Elastic und Metriken. CloudWatch

`AmazonDocDBElasticReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDocDBElasticReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Juni 2023, 14:37 UTC
- Bearbeitete Zeit: 21. Juni 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DocumentDB mit MongoDB-Kompatibilität. Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos sowie vollen Zugriff auf Amazon RDS und Amazon Neptune gewährt.

`AmazonDocDBFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDocDBFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Januar 2019, 20:21 UTC
- Bearbeitete Zeit: 9. Januar 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon DocumentDB mit MongoDB-Kompatibilität. Beachten Sie, dass diese Richtlinie auch Zugriff auf Amazon RDS- und Amazon Neptune Neptune-Ressourcen gewährt.

`AmazonDocDBReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDocDBReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Januar 2019, 20:30 Uhr UTC
- Bearbeitungszeit: 9. Januar 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDRSVPCManagement

Beschreibung: Bietet Zugriff auf die Verwaltung der VPC-Einstellungen für von Amazon verwaltete Kundenkonfigurationen

`AmazonDRSVPCManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDRSVPCManagement` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. September 2015, 00:09 Uhr UTC
- Zeit bearbeitet: 2. September 2015, 00:09 Uhr UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDynamoDBFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DynamoDB über die. AWS Management Console

`AmazonDynamoDBFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDynamoDBFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 29. Januar 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDynamoDBFullAccesswithDataPipeline

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/DynamoDBPipeline.html. Bietet vollen Zugriff auf Amazon DynamoDB, einschließlich Export/Import mithilfe AWS der Data Pipeline über die. AWS Management Console

`AmazonDynamoDBFullAccesswithDataPipeline`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDynamoDBFullAccesswithDataPipeline` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 12. November 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDynamoDBReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon DynamoDB über die. AWS Management Console

`AmazonDynamoDBReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonDynamoDBReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 20. März 2024, 15:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
```

```
        "dynamodb:List*",
        "dynamodb:GetItem",
        "dynamodb:GetResourcePolicy",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dax:Describe*",
        "dax:List*",
        "dax:GetItem",
        "dax:BatchGetItem",
        "dax:Query",
        "dax:Scan",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:GetFunctionConfiguration",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CCIAccess",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEBSCSIDriverPolicy

Beschreibung: IAM-Richtlinie, die es dem CSI-Treiberdienstkonto ermöglicht, in Ihrem Namen Anrufe an verwandte Dienste wie EC2 zu tätigen.

`AmazonEBSCSIDriverPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEBSCSIDriverPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. April 2022, 17:24 UTC
- Zeit bearbeitet: 18. November 2022, 14:42 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerRegistryFullAccess

Beschreibung: Bietet administrativen Zugriff auf Amazon ECR-Ressourcen

`AmazonEC2ContainerRegistryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2ContainerRegistryFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Dezember 2015, 17:06 UTC
- Bearbeitete Zeit: 5. Dezember 2020, 00:04 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerRegistryPowerUser

Beschreibung: Bietet vollen Zugriff auf Amazon EC2 Container Registry-Repositorys, erlaubt jedoch weder das Löschen von Repositorys noch Richtlinienänderungen.

`AmazonEC2ContainerRegistryPowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2ContainerRegistryPowerUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Dezember 2015, 17:05 UTC
- Bearbeitete Zeit: 10. Dezember 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerRegistryReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EC2 Container Registry-Repositorys.

`AmazonEC2ContainerRegistryReadOnly`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2ContainerRegistryReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Dezember 2015, 17:04 UTC
- Bearbeitete Zeit: 10. Dezember 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerServiceAutoscaleRole

Beschreibung: Richtlinie zur Aktivierung von Task Autoscaling für Amazon EC2 Container Service

`AmazonEC2ContainerServiceAutoscaleRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2ContainerServiceAutoscaleRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. Mai 2016, 23:25 Uhr UTC
- Bearbeitete Zeit: 5. Februar 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerServiceEventsRole

Beschreibung: Richtlinie zur Aktivierung von CloudWatch Ereignissen für den EC2 Container Service

`AmazonEC2ContainerServiceEventsRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2ContainerServiceEventsRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 30. Mai 2017, 16:51 UTC
- Bearbeitete Zeit: 06. März 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerServiceforEC2Role

Beschreibung: Standardrichtlinie für die Amazon EC2-Rolle für Amazon EC2 Container Service.

`AmazonEC2ContainerServiceforEC2Role`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2ContainerServiceforEC2Role` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. März 2015, 18:45 Uhr UTC
- Bearbeitete Zeit: 6. März 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerServiceRole

Beschreibung: Standardrichtlinie für die Amazon ECS-Servicerolle.

`AmazonEC2ContainerServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2ContainerServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. April 2015, 16:14 UTC
- Bearbeitete Zeit: 11. August 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2FullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EC2 über die AWS Management Console.

`AmazonEC2FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 27. November 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EC2 über die AWS Management Console.

`AmazonEC2ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 14. Februar 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RoleforAWSCodeDeploy

Beschreibung: Ermöglicht EC2-Zugriff auf den S3-Bucket zum Herunterladen der Revision. Diese Rolle wird vom CodeDeploy Agenten auf EC2-Instances benötigt.

`AmazonEC2RoleforAWSCodeDeploy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2RoleforAWSCodeDeploy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. Mai 2015, 18:10 Uhr UTC
- Bearbeitete Zeit: 20. März 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RoleforAWSCodeDeployLimited

Beschreibung: Bietet eingeschränkten EC2-Zugriff auf den S3-Bucket zum Herunterladen der Revision. Diese Rolle wird vom CodeDeploy Agenten auf EC2-Instances benötigt.

`AmazonEC2RoleforAWSCodeDeployLimited`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2RoleforAWSCodeDeployLimited` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. August 2020, 17:55 Uhr UTC
- Bearbeitete Zeit: 20. Januar 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RoleforDataPipelineRole

Beschreibung: Standardrichtlinie für die Servicerolle Amazon EC2 Role for Data Pipeline.

`AmazonEC2RoleforDataPipelineRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2RoleforDataPipelineRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 22. Februar 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RoleforSSM

Beschreibung: Diese Richtlinie wird bald veraltet sein. Bitte verwenden Sie die ManagedInstanceCore AmazonSSM-Richtlinie, um die Kernfunktionen des AWS Systems Manager Manager-Service auf EC2-Instances zu aktivieren. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/systems-manager/latest/userguide/ .html setup-instance-profile

`AmazonEC2RoleforSSM`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2RoleforSSM` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. Mai 2015, 17:48 Uhr UTC
- Bearbeitete Zeit: 24. Januar 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RolePolicyForLaunchWizard

Beschreibung: Verwaltete Richtlinie für die LaunchWizard Amazon-Servicerolle für EC2

`AmazonEC2RolePolicyForLaunchWizard`dist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2RolePolicyForLaunchWizard` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 08:05 UTC
- Bearbeitete Zeit: 16. Mai 2022, 21:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
```

```
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeRouteTables",
        "ec2:ModifyInstanceAttribute",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricData",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LaunchWizardResourceGroupID",
            "LaunchWizardApplicationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:Create*",
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
```

```
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteTable",
        "dynamodb:CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:dynamodb:*:*:table/LaunchWizard*",
        "arn:aws:sqs:*:*:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2SpotFleetAutoscaleRole

Beschreibung: Richtlinie zur Aktivierung von Autoscaling für Amazon EC2 Spot Fleet

`AmazonEC2SpotFleetAutoscaleRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2SpotFleetAutoscaleRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. August 2016, 18:27 Uhr UTC
- Bearbeitete Zeit: 18. Februar 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2SpotFleetTaggingRole

Beschreibung: Ermöglicht EC2 Spot Fleet, Spot-Instances in Ihrem Namen anzufordern, zu beenden und zu kennzeichnen.

`AmazonEC2SpotFleetTaggingRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEC2SpotFleetTaggingRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. Juni 2017, 18:19 Uhr UTC
- Bearbeitete Zeit: 23. April 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECS_FullAccess

Beschreibung: Bietet administrativen Zugriff auf Amazon ECS-Ressourcen und ermöglicht ECS-Funktionen durch Zugriff auf andere AWS Serviceressourcen, einschließlich VPCs, Auto Scaling Scaling-Gruppen und CloudFormation Stacks.

`AmazonECS_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonECS_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. November 2017, 21:36 UTC
- Bearbeitete Zeit: 4. Januar 2023, 16:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Version der Richtlinie

Richtlinienversion: v20 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
```

```
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:ListMeshes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:Describe*",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ContinueDeployment",
        "codedeploy:CreateApplication",
        "codedeploy:CreateDeployment",
        "codedeploy:CreateDeploymentGroup",
        "codedeploy:GetApplication",
        "codedeploy:GetApplicationRevision",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:ListApplicationRevisions",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
```

```
        "codedeploy:RegisterApplicationRevision",
        "codedeploy:StopDeployment",
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateInternetGateway",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RequestSpotFleet",
        "ec2:RunInstances",
        "ecs:*",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
```

```
        "events:RemoveTargets",
        "fsx:DescribeFileSystems",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "lambda:ListFunctions",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:FilterLogEvents",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "servicediscovery:CreatePrivateDnsNamespace",
        "servicediscovery:CreateService",
        "servicediscovery:DeleteService",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetOperation",
        "servicediscovery:GetService",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:UpdateService",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteInternetGateway",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
```

```
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsAutoscaleRole*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com",
            "ecs.application-autoscaling.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateTargetGroup",
            "CreateRule",
            "CreateListener",
            "CreateLoadBalancer"
          ]
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

Beschreibung: Bietet Administratorzugriff auf Private Certificate Authority, AWS Secrets Manager und andere, die für die Verwaltung der TLS-Funktionen von ECS Service Connect in Ihrem Namen AWS-Services erforderlich sind.

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. Januar 2024, 20:08 UTC
- Bearbeitete Zeit: 19. Januar 2024, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSInfrastructureRolePolicyForVolumes

Beschreibung: Ermöglicht den Zugriff auf andere AWS Serviceressourcen, die für die Verwaltung von Volumes im Zusammenhang mit ECS-Workloads in Ihrem Namen erforderlich sind.

`AmazonECSInfrastructureRolePolicyForVolumes`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonECSInfrastructureRolePolicyForVolumes` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. Januar 2024, 22:56 UTC
- Bearbeitete Zeit: 10. Januar 2024, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSServiceRolePolicy

Beschreibung: Richtlinie, um Amazon ECS die Verwaltung Ihres Clusters zu ermöglichen.

`AmazonECSServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. Oktober 2017, 01:18 Uhr UTC
- Bearbeitete Zeit: 4. Dezember 2023, 19:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:Get*",
        "route53:List*",
        "route53:UpdateHealthCheck",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:UpdateInstanceCustomHealthStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
```

```
      "Action" : [
        "autoscaling:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:RecordLifecycleActionHeartbeat"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "autoscaling:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "AutoScalingPlanManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling-plans:CreateScalingPlan",
        "autoscaling-plans:DeleteScalingPlan",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:DescribeScalingPlanResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
```

```
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CWAlarmManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ECSTagging",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "CWLogGroupManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
    },
    {
```

```
      "Sid" : "CWLogStreamManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
    },
    {
      "Sid" : "ExecuteCommandSessionManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExecuteCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*",
        "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
      ]
    },
    {
      "Sid" : "CloudMapResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:CreateHttpNamespace",
        "servicediscovery:CreateService"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonECSManaged"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "CloudMapResourceTagging",
      "Effect" : "Allow",
      "Action" : "servicediscovery:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonECSManaged" : "*"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDeletion",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DeleteService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSTaskExecutionRolePolicy

Beschreibung: Bietet Zugriff auf andere AWS Serviceressourcen, die für die Ausführung von Amazon ECS-Aufgaben erforderlich sind

`AmazonECSTaskExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonECSTaskExecutionRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 16. November 2017, 18:48 Uhr UTC
- Zeit bearbeitet: 16. November 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEFSCSIDriverPolicy

Beschreibung: Bietet Verwaltungszugriff auf EFS-Ressourcen und Lesezugriff auf EC2

`AmazonEFSCSIDriverPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEFSCSIDriverPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. Juli 2023, 20:10 UTC
- Bearbeitete Zeit: 25. Juli 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKS_CNI_Policy

Beschreibung: Diese Richtlinie gewährt dem Amazon VPC CNI Plugin (amazon-vpc-cni-k8s) die erforderlichen Berechtigungen, um die IP-Adresskonfiguration auf Ihren EKS-Worker-Knoten zu ändern. Dieser Berechtigungssatz ermöglicht es dem CNI, Elastic Network Interfaces in Ihrem Namen aufzulisten, zu beschreiben und zu ändern. Weitere Informationen zum AWS VPC CNI Plugin finden Sie hier: https://github.com/aws/ 8s amazon-vpc-cni-k

`AmazonEKS_CNI_Policy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEKS_CNI_Policy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:07 UTC
- Bearbeitete Zeit: 4. März 2024, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSClusterPolicy

Beschreibung: Diese Richtlinie gewährt Kubernetes die erforderlichen Berechtigungen, um Ressourcen in Ihrem Namen zu verwalten. Kubernetes benötigt Ec2: CreateTags -Berechtigungen, um identifizierende Informationen auf EC2-Ressourcen zu platzieren, einschließlich, aber nicht beschränkt auf Instances, Sicherheitsgruppen und Elastic Network Interfaces.

`AmazonEKSClusterPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEKSClusterPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:06 UTC
- Bearbeitete Zeit: 7. Februar 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "autoscaling:UpdateAutoScalingGroup",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteRoute",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyVolume",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
```

```
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSConnectorServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht Amazon EKS die Verwaltung von AWS Ressourcen für den EKS-Connector

`AmazonEKSConnectorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. September 2021, 20:31 UTC
- Bearbeitete Zeit: 4. September 2021, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "ssm:CreateActivation",
        "ssm:DescribeInstanceInformation",
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*::document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutManagedEventRule",
```

```
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com",
          "events:source" : "aws.ssm"
        }
      }
    },
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSFargatePodExecutionRolePolicy

Beschreibung: Bietet Zugriff auf andere AWS Serviceressourcen, die für die Ausführung von Amazon EKS-Pods auf AWS Fargate erforderlich sind

`AmazonEKSFargatePodExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEKSFargatePodExecutionRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. November 2019, 04:34 UTC
- Bearbeitete Zeit: 22. November 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSForFargateServiceRolePolicy

Beschreibung: Diese Richtlinie gewährt Amazon EKS die erforderlichen Berechtigungen zur Ausführung von Fargate-Aufgaben.

`AmazonEKSForFargateServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. November 2019, 04:36 Uhr UTC
- Bearbeitete Zeit: 22. November 2019, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSLocalOutpostClusterPolicy

Beschreibung: Diese Richtlinie gewährt den Kontrollebeneninstanzen des lokalen EKS-Clusters, die in Ihrem Konto ausgeführt werden, Berechtigungen, um Ressourcen in Ihrem Namen zu verwalten.

`AmazonEKSLocalOutpostClusterPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEKSLocalOutpostClusterPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 24. August 2022, 21:56 UTC
- Bearbeitete Zeit: 17. Oktober 2022, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:DescribeInstanceProperties",
        "ssm:DescribeDocumentParameters",
        "ssm:ListInstanceAssociations",
        "ssm:RegisterManagedInstance",
        "ssm:UpdateInstanceInformation",
```

```
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:PutComplianceItems",
        "ssm:PutInventory",
        "ecr-public:GetAuthorizationToken",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/eks/*",
        "arn:aws:ecr:*:*:repository/bottlerocket-admin",
        "arn:aws:ecr:*:*:repository/bottlerocket-control-eks",
        "arn:aws:ecr:*:*:repository/diagnostics-collector-eks",
        "arn:aws:ecr:*:*:repository/kubelet-config-updater"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSLocalOutpostServiceRolePolicy

Beschreibung: Ermöglicht Amazon EKS Local, AWS Dienste in Ihrem Namen anzurufen.

`AmazonEKSLocalOutpostServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. August 2022, 21:53 UTC
- Bearbeitete Zeit: 24. Oktober 2022, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribePlacementGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DeleteSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DescribeSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
```

```
          "ssm:resourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*::document/AmazonEKS-ControlPlaneInstanceProxy"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
        "ssm:TerminateSession"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSServicePolicy

Beschreibung: Diese Richtlinie ermöglicht es Amazon Elastic Container Service for Kubernetes, die für den Betrieb von EKS-Clustern erforderlichen Ressourcen zu erstellen und zu verwalten.

`AmazonEKSServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEKSServicePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:08 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
```

```
        "eks:UpdateClusterVersion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSServiceRolePolicy

Beschreibung: Eine serviceverknüpfte Rolle ist erforderlich, damit Amazon EKS AWS Services in Ihrem Namen anrufen kann.

`AmazonEKSServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Februar 2020, 20:10 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateNetworkInterfacePermission",
        "iam:ListAttachedRolePolicies",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "ec2:ResourceTag/Name" : "eks-cluster-sg*"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ],
          "aws:RequestTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSVPCResourceController

Beschreibung: Richtlinie, die vom VPC Resource Controller zur Verwaltung von ENI und IPs für Worker-Knoten verwendet wird.

`AmazonEKSVPCResourceController`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEKSVPCResourceController` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. August 2020, 00:55 UTC
- Zeit bearbeitet: 12. August 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSWorkerNodePolicy

Beschreibung: Diese Richtlinie ermöglicht es Amazon EKS-Worker-Knoten, sich mit Amazon EKS-Clustern zu verbinden.

`AmazonEKSWorkerNodePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEKSWorkerNodePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:09 UTC
- Bearbeitete Zeit: 27. November 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElastiCacheFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon ElastiCache über die AWS Management Console.

`AmazonElastiCacheFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElastiCacheFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 28. November 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElastiCacheReadOnlyAccess

Beschreibung: Bietet Nur-Lesezugriff auf Amazon ElastiCache über die AWS Management Console.

`AmazonElastiCacheReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElastiCacheReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Action" : [
        "elasticache:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticContainerRegistryPublicFullAccess

Beschreibung: Bietet administrativen Zugriff auf öffentliche Ressourcen von Amazon ECR

`AmazonElasticContainerRegistryPublicFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticContainerRegistryPublicFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 17:25 Uhr UTC
- Zeit bearbeitet: 1. Dezember 2020, 17:25 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticContainerRegistryPublicPowerUser

Beschreibung: Bietet vollen Zugriff auf öffentliche Amazon ECR-Repositorys, erlaubt jedoch nicht das Löschen von Repositorys oder Richtlinienänderungen.

`AmazonElasticContainerRegistryPublicPowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticContainerRegistryPublicPowerUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 16:16 UTC
- Zeit bearbeitet: 1. Dezember 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticContainerRegistryPublicReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf öffentliche Amazon ECR-Repositorys.

`AmazonElasticContainerRegistryPublicReadOnly`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticContainerRegistryPublicReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 17:27 UTC
- Zeit bearbeitet: 1. Dezember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemClientFullAccess

Beschreibung: Bietet Root-Client-Zugriff auf ein Amazon EFS-Dateisystem

`AmazonElasticFileSystemClientFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticFileSystemClientFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Januar 2020, 16:27 UTC
- Bearbeitete Zeit: 13. Januar 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemClientReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Client-Zugriff auf ein Amazon EFS-Dateisystem

`AmazonElasticFileSystemClientReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticFileSystemClientReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Januar 2020, 16:24 UTC
- Bearbeitete Zeit: 13. Januar 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemClientReadWriteAccess

Beschreibung: Bietet Lese- und Schreibclientzugriff auf ein Amazon EFS-Dateisystem

`AmazonElasticFileSystemClientReadWriteAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticFileSystemClientReadWriteAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Januar 2020, 16:21 UTC
- Bearbeitete Zeit: 13. Januar 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EFS über die AWS Management Console.

`AmazonElasticFileSystemFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticFileSystemFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2015, 16:22 UTC
- Bearbeitete Zeit: 28. November 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "elasticfilesystem:DeleteTags",
        "elasticfilesystem:DeleteAccessPoint",
        "elasticfilesystem:DeleteFileSystemPolicy",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ModifyMountTargetSecurityGroups",
        "elasticfilesystem:PutAccountPreferences",
        "elasticfilesystem:PutBackupPolicy",
        "elasticfilesystem:PutLifecycleConfiguration",
        "elasticfilesystem:PutFileSystemPolicy",
        "elasticfilesystem:UpdateFileSystem",
        "elasticfilesystem:UpdateFileSystemProtection",
        "elasticfilesystem:TagResource",
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:Backup",
        "elasticfilesystem:Restore",
        "kms:DescribeKey",
```

```
        "kms:ListAliases"
      ],
      "Sid" : "ElasticFileSystemFullAccess",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Sid" : "CreateServiceLinkedRoleForEFS",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticfilesystem.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EFS über die AWS Management Console.

`AmazonElasticFileSystemReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticFileSystemReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2015, 16:25 UTC
- Bearbeitete Zeit: 10. Januar 2022, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
```

```
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ListTagsForResource",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemServiceRolePolicy

Beschreibung: Ermöglicht Amazon Elastic File System, AWS Ressourcen in Ihrem Namen zu verwalten

`AmazonElasticFileSystemServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 5. November 2019, 16:52 UTC
- Bearbeitete Zeit: 10. Januar 2022, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-plan:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DeleteReplicationConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemsUtils

Beschreibung: Ermöglicht Kunden, AWS Systems Manager zu verwenden, um das Paket Amazon EFS Utilities (amazon-efs-utils) auf ihren EC2-Instances automatisch zu verwalten und Benachrichtigungen über Erfolgs- und CloudWatchLog Fehlschläge beim Einhängen des EFS-Dateisystems zu erhalten.

`AmazonElasticFileSystemsUtils`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticFileSystemsUtils` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 29. September 2020, 15:16 Uhr UTC
- Bearbeitete Zeit: 29. September 2020, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceEditorsRole

Beschreibung: Standardrichtlinie für die Amazon Elastic MapReduce Editors-Servicerolle.

`AmazonElasticMapReduceEditorsRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticMapReduceEditorsRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 16. November 2018, 21:55 UTC
- Bearbeitete Zeit: 9. Februar 2023, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

```
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceforAutoScalingRole

Beschreibung: Amazon Elastic MapReduce für Auto Scaling. Rolle, mit der Auto Scaling Instances zu Ihrem EMR-Cluster hinzufügen und daraus entfernen kann.

`AmazonElasticMapReduceforAutoScalingRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticMapReduceforAutoScalingRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 18. November 2016, 01:09 UTC
- Bearbeitete Zeit: 18. November 2016, 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceforEC2Role

Beschreibung: Standardrichtlinie für die Servicerolle Amazon Elastic MapReduce for EC2.

`AmazonElasticMapReduceforEC2Role`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticMapReduceforEC2Role` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 11. August 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceFullAccess

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html. Bietet vollen Zugriff auf Amazon Elastic MapReduce und die dafür benötigten zugrunde liegenden Services wie EC2 und S3

`AmazonElasticMapReduceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticMapReduceFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 11. Oktober 2019, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReducePlacementGroupPolicy

Beschreibung: Richtlinie, die es EMR ermöglicht, EC2-Platzierungsgruppen zu erstellen, zu beschreiben und zu löschen.

`AmazonElasticMapReducePlacementGroupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticMapReducePlacementGroupPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. September 2020, 00:37 UTC
- Zeit bearbeitet: 29. September 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Elastic MapReduce über die AWS Management Console.

`AmazonElasticMapReduceReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticMapReduceReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 29. Juli 2020, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceRole

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-managed-iam-policies.html. Standardrichtlinie für die Amazon MapReduce Elastic-Servicerolle.

`AmazonElasticMapReduceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticMapReduceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 24. Juni 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticsearchServiceRolePolicy

Beschreibung: Erlauben Sie Amazon Elasticsearch Service, in Ihrem Namen auf andere AWS Services wie EC2 Networking APIs zuzugreifen.

`AmazonElasticsearchServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Juli 2017, 00:15 UTC
- Bearbeitete Zeit: 23. Oktober 2023, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticTranscoder_FullAccess

Beschreibung: Gewährt Benutzern vollen Zugriff auf Elastic Transcoder und den Zugriff auf zugehörige Dienste, der für die volle Funktionalität von Elastic Transcoder erforderlich ist.

`AmazonElasticTranscoder_FullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticTranscoder_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. April 2018, 18:59 Uhr UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticTranscoder_JobsSubmitter

Beschreibung: Erteilt Benutzern die Erlaubnis, Voreinstellungen zu ändern, Jobs einzureichen und Elastic Transcoder Transcoder-Einstellungen einzusehen. Diese Richtlinie gewährt auch einen gewissen Lesezugriff auf einige andere Dienste, die für die Nutzung der Elastic Transcode-Konsole erforderlich sind, darunter S3, IAM und SNS.

`AmazonElasticTranscoder_JobsSubmitter`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticTranscoder_JobsSubmitter` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 7. Juni 2018, 21:12 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticTranscoder_ReadOnlyAccess

Beschreibung: Gewährt Benutzern nur Lesezugriff auf Elastic Transcoder und Listenzugriff auf verwandte Dienste.

`AmazonElasticTranscoder_ReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticTranscoder_ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Juni 2018, 21:09 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticTranscoderRole

Beschreibung: Standardrichtlinie für die Amazon Elastic Transcoder-Servicerolle.

`AmazonElasticTranscoderRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonElasticTranscoderRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC

- Bearbeitete Zeit: 13. Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRCleanupPolicy

Beschreibung: Ermöglicht die Aktionen, die EMR zum Beenden und Löschen von AWS EC2-Ressourcen benötigt, wenn die EMR-Dienstrolle diese Fähigkeit verloren hat.

`AmazonEMRCleanupPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. September 2017, 23:54 Uhr UTC
- Bearbeitete Zeit: 29. September 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRContainersServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf andere AWS Serviceressourcen, die für die Ausführung von Amazon EMR erforderlich sind

`AmazonEMRContainersServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. Dezember 2020, 00:38 UTC
- Bearbeitete Zeit: 10. März 2023, 22:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRFullAccessPolicy_v2

Beschreibung: Bietet vollen Zugriff auf Amazon EMR

`AmazonEMRFullAccessPolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEMRFullAccessPolicy_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. März 2021, 01:50 UTC
- Bearbeitete Zeit: 28. Juli 2023, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:CreateEditor",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteEditor",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ModifyCluster",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:ModifyInstanceGroups",
        "elasticmapreduce:OpenEditorInConsole",
```

```
        "elasticmapreduce:PutAutoScalingPolicy",
        "elasticmapreduce:PutBlockPublicAccessConfiguration",
        "elasticmapreduce:PutManagedScalingPolicy",
        "elasticmapreduce:RemoveAutoScalingPolicy",
        "elasticmapreduce:RemoveManagedScalingPolicy",
        "elasticmapreduce:RemoveTags",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:StartEditor",
        "elasticmapreduce:StopEditor",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleForElasticMapReduce",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_DefaultRole_V2",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticmapreduce.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
```

```
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticmapreduce.amazonaws.com*/AWSServiceRoleForEMRCleanup*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleUIActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "iam:ListRoles"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRReadOnlyAccessPolicy_v2

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EMR und die zugehörigen CloudWatch Metriken.

`AmazonEMRReadOnlyAccessPolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEMRReadOnlyAccessPolicy_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. März 2021, 01:39 UTC
- Bearbeitete Zeit: 2. August 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRServerlessServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf andere AWS Serviceressourcen, die für die Ausführung von Amazon EMRServerless erforderlich sind

`AmazonEMRServerlessServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Mai 2022, 23:15 UTC
- Bearbeitete Zeit: 25. Januar 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRServicePolicy_v2

Beschreibung: Diese Richtlinie wird für die Amazon EMR-Servicerolle verwendet und sollte NICHT für andere IAM-Benutzer oder -Rollen in Ihrem Konto verwendet werden. Die Richtlinie gewährt Berechtigungen zum Erstellen und Verwalten von Ressourcen im Zusammenhang mit EMR und verwandten Diensten, die für den Betrieb Ihres EMR-Clusters erforderlich sind.

`AmazonEMRServicePolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEMRServicePolicy_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. März 2021, 01:11 Uhr UTC
- Bearbeitete Zeit: 02. Mai 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonESCognitoAccess

Beschreibung: Bietet eingeschränkten Zugriff auf den Amazon Cognito Cognito-Konfigurationsservice.

`AmazonESCognitoAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonESCognitoAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Februar 2018, 22:29 UTC
- Bearbeitete Zeit: 20. Dezember 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonESFullAccess

Beschreibung: Bietet vollen Zugriff auf den Amazon ES-Konfigurationsservice.

`AmazonESFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonESFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Oktober 2015, 19:14 UTC
- Zeit bearbeitet: 1. Oktober 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonESReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Amazon ES-Konfigurationsservice.

`AmazonESReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonESReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Oktober 2015, 19:18 UTC
- Bearbeitete Zeit: 3. Oktober 2018, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeApiDestinationsServiceRolePolicy

Beschreibung: Ermöglicht EventBridge den Zugriff auf Secret Manager-Ressourcen in Ihrem Namen.

`AmazonEventBridgeApiDestinationsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 11. Februar 2021, 20:52 UTC
- Bearbeitete Zeit: 11. Februar 2021, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EventBridge.

`AmazonEventBridgeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEventBridgeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Juli 2019, 14:08 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleAccessForEventBridge",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgePipesFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EventBridge Pipes.

`AmazonEventBridgePipesFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEventBridgePipesFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2022, 17:03 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgePipesOperatorAccess

Beschreibung: Bietet schreibgeschützten Zugriff und Bedienerzugriff (Fähigkeit, Pipes zu beenden und zu starten) auf Amazon EventBridge Pipes.

`AmazonEventBridgePipesOperatorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEventBridgePipesOperatorAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2022, 17:04 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgePipesReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EventBridge Pipes.

`AmazonEventBridgePipesReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEventBridgePipesReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2022, 17:04 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon EventBridge.

`AmazonEventBridgeReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEventBridgeReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Juli 2019, 13:59 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchedulerFullAccess

Beschreibung: Die AmazonEventBridgeSchedulerFullAccess verwaltete Richtlinie gewährt Berechtigungen zur Verwendung aller EventBridge Scheduler-Aktionen für Zeitpläne und Zeitplangruppen.

`AmazonEventBridgeSchedulerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEventBridgeSchedulerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2022, 18:37 UTC
- Zeit bearbeitet: 10. November 2022, 18:37 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchedulerReadOnlyAccess

Beschreibung: Die AmazonEventBridgeSchedulerReadOnlyAccess verwaltete Richtlinie gewährt nur Leseberechtigungen zum Anzeigen von Details zu Ihren Zeitplänen und Zeitplangruppen

`AmazonEventBridgeSchedulerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEventBridgeSchedulerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2022, 18:50 UTC
- Bearbeitete Zeit: 10. November 2022, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchemasFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEventBridgeSchemasFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2019, 23:12 Uhr UTC
- Zeit bearbeitet: 28. November 2019, 23:12 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchemasReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonEventBridgeSchemasReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2019, 23:05 UTC
- Bearbeitete Zeit: 1. Mai 2020, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchemasServiceRolePolicy

Beschreibung: Erteilt Berechtigungen für verwaltete Regeln, die von EventBridge Amazon-Schemas erstellt wurden.

`AmazonEventBridgeSchemasServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. November 2019, 01:10 Uhr UTC
- Bearbeitete Zeit: 27. November 2019, 01:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFISServiceRolePolicy

Beschreibung: Richtlinie, die es der AWS FIS ermöglicht, die Überwachung und die Auswahl der Ressourcen für Experimente zu verwalten.

`AmazonFISServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Dezember 2020, 21:18 Uhr UTC

- Bearbeitete Zeit: 25. Oktober 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonForecastFullAccess

Beschreibung: Ermöglicht den Zugriff auf alle Aktionen für Amazon Forecast

`AmazonForecastFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonForecastFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2019, 01:52 UTC
- Bearbeitete Zeit: 18. Januar 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFraudDetectorFullAccessPolicy

Beschreibung: Ermöglicht den Zugriff auf alle Aktionen für Amazon Fraud Detector

`AmazonFraudDetectorFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonFraudDetectorFullAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 03. Dezember 2019, 22:46 Uhr UTC
- Bearbeitete Zeit: 3. Dezember 2019, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFreeRTOSFullAccess

Beschreibung: Vollständige Zugriffsrichtlinie für Amazon FreeRTOS

`AmazonFreeRTOSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonFreeRTOSFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 15:32 UTC
- Zeit bearbeitet: 29. November 2017, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFreeRTOSOTAUpdate

Beschreibung: Ermöglicht dem Benutzer den Zugriff auf Amazon FreeRTOS OTA Update

`AmazonFreeRTOSOTAUpdate`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonFreeRTOSOTAUpdate` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. August 2018, 22:43 UTC
- Bearbeitete Zeit: 18. Dezember 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon FSx und Zugriff auf verwandte AWS Dienste über die AWS Management Console.

`AmazonFSxConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonFSxConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:36 UTC
- Bearbeitete Zeit: 10. Januar 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
```

```
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateFSxSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
```

```
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxConsoleReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon FSx und Zugriff auf verwandte AWS Dienste über die AWS Management Console.

`AmazonFSxConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonFSxConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:35 UTC
- Bearbeitete Zeit: 10. Januar 2024, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon FSx und Zugriff auf verwandte AWS Dienste.

`AmazonFSxFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonFSxFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:34 UTC
- Bearbeitete Zeit: 10. Januar 2024, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
```

```
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
      ]
    },
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon FSx.

`AmazonFSxReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonFSxReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:33 UTC
- Zeit bearbeitet: 28. November 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxServiceRolePolicy

Beschreibung: Ermöglicht Amazon FSx, AWS Ressourcen in Ihrem Namen zu verwalten

`AmazonFSxServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 28. November 2018, 10:38 UTC
- Bearbeitete Zeit: 10. Januar 2024, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "PutMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/FSx"
        }
      }
    },
    {
      "Sid" : "TagResourceNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonFSx.FileSystemId"
        }
      }
    },
    {
      "Sid" : "ManageNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
        }
      }
    },
    {
      "Sid" : "ManageRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
    },
    {
      "Sid" : "ManageAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
  ]
```

```
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGlacierFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Glacier über die AWS Management Console.

`AmazonGlacierFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonGlacierFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGlacierReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Glacier über die AWS Management Console.

`AmazonGlacierReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonGlacierReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 5. Mai 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGrafanaAthenaAccess

Beschreibung: Diese Richtlinie gewährt Zugriff auf Amazon Athena und die Abhängigkeiten, die erforderlich sind, um das Abfragen und Schreiben von Ergebnissen aus dem Amazon Athena-Plugin in Amazon Grafana in S3 zu ermöglichen.

`AmazonGrafanaAthenaAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonGrafanaAthenaAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. November 2021, 17:11 Uhr UTC
- Bearbeitete Zeit: 22. November 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGrafanaCloudWatchAccess

Beschreibung: Diese Richtlinie gewährt Zugriff auf Amazon CloudWatch und die Abhängigkeiten, die für die Verwendung CloudWatch als Datenquelle in Amazon Managed Grafana erforderlich sind.

`AmazonGrafanaCloudWatchAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonGrafanaCloudWatchAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. März 2023, 22:41 UTC
- Bearbeitete Zeit: 24. März 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGrafanaRedshiftAccess

Beschreibung: Diese Richtlinie gewährt begrenzten Zugriff auf Amazon Redshift und die Abhängigkeiten, die für die Verwendung des Amazon Redshift Redshift-Plug-ins in Amazon Grafana erforderlich sind.

`AmazonGrafanaRedshiftAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonGrafanaRedshiftAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. November 2021, 23:15 Uhr UTC
- Bearbeitete Zeit: 26. November 2021, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGrafanaServiceLinkedRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von Amazon Grafana verwaltet oder verwendet werden.

`AmazonGrafanaServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. November 2022, 23:10 UTC
- Zeit bearbeitet: 8. November 2022, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyFullAccess

Beschreibung: Bietet vollen Zugriff auf die Nutzung von Amazon GuardDuty.

`AmazonGuardDutyFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonGuardDutyFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2017, 22:31 UTC
- Bearbeitete Zeit: 10. Juni 2024, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
```

```
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamGetRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtectionPlan",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection-plan.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Beschreibung: Der GuardDuty Malware-Schutz verwendet die mit dem Namen verknüpfte Rolle (Service Linked Role, SLR). AWSServiceRoleForAmazonGuardDutyMalwareProtection Diese dienstbezogene Rolle ermöglicht es dem GuardDuty Malware-Schutz, Scans ohne Agenten durchzuführen, um Malware zu erkennen. Sie GuardDuty ermöglicht das Erstellen von Snapshots in Ihrem Konto und das Teilen der Snapshots mit dem GuardDuty Dienstkonto, um nach Malware zu suchen. Es wertet diese gemeinsam genutzten Snapshots aus und bezieht die abgerufenen EC2-Instanz-Metadaten in die Ergebnisse des Malware-Schutzes ein. GuardDuty Die mit dem AWSServiceRoleForAmazonGuardDutyMalwareProtection Dienst verknüpfte Rolle vertraut darauf, dass der Service malware protection.guardduty.amazonaws.com die Rolle übernimmt.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Juli 2022, 19:06 UTC
- Bearbeitete Zeit: 25. Januar 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf GuardDuty Amazon-Ressourcen

`AmazonGuardDutyReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonGuardDutyReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2017, 22:29 UTC
- Bearbeitete Zeit: 16. November 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyServiceRolePolicy

Beschreibung: Ermöglichen Sie den Zugriff auf AWS Ressourcen, die von Amazon Guard Duty verwendet oder verwaltet werden

`AmazonGuardDutyServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 28. November 2017, 20:12 Uhr UTC
- Bearbeitete Zeit: 27. März 2024, 00:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        },
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.guardduty-data",
            "com.amazonaws.*.guardduty-data-fips"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutySecurityGroupManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/GuardDutyManaged" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateEksAddonPolicy",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEksAddonManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
    },
```

```
    {
      "Sid" : "GuardDutyEksClusterTagResourcePolicy",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
      "Effect" : "Allow",
      "Action" : "ecs:PutAccountSettingDefault",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:account-setting" : [
            "guardDutyActivate"
          ]
        }
      }
    },
    {
      "Sid" : "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation",
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmAddTagsToResourcePermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyManaged"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmCreateUpdateAssociationInstanceDocumentPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
    },
    {
      "Sid" : "SsmSendCommandPermission",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin"
      ]
    },
    {
      "Sid" : "SsmGetCommandStatus",
      "Effect" : "Allow",
      "Action" : "ssm:GetCommandInvocation",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHealthLakeFullAccess

Beschreibung: Bietet vollen Zugriff auf den HealthLake Amazon-Service.

`AmazonHealthLakeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonHealthLakeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Februar 2021, 01:07 UTC
- Bearbeitete Zeit: 17. Februar 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHealthLakeReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf den HealthLake Amazon-Service.

`AmazonHealthLakeReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonHealthLakeReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Februar 2021, 02:43 UTC
- Bearbeitete Zeit: 17. Februar 2021, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeFullAccess

Beschreibung: Bietet vollen Zugriff auf Honeycode über das AWS Management Console und das SDK.

`AmazonHoneycodeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonHoneycodeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 24. Juni 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Honeycode über das AWS Management Console und das SDK.

`AmazonHoneycodeReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonHoneycodeReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeServiceRolePolicy

Beschreibung: Für Amazon Honeycode ist eine servicebezogene Rolle erforderlich, um auf Ihre Ressourcen zugreifen zu können.

`AmazonHoneycodeServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2020, 18:03 UTC
- Zeit bearbeitet: 18. November 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeTeamAssociationFullAccess

Beschreibung: Bietet vollen Zugriff auf Honeycode Team Association über das AWS Management Console und das SDK.

`AmazonHoneycodeTeamAssociationFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonHoneycodeTeamAssociationFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 24. Juni 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeTeamAssociationReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Honeycode Team Association über das AWS Management Console und das SDK.

`AmazonHoneycodeTeamAssociationReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonHoneycodeTeamAssociationReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:27 UTC
- Bearbeitete Zeit: 24. Juni 2020, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeWorkbookFullAccess

Beschreibung: Bietet vollen Zugriff auf Honeycode Workbook über das AWS Management Console und das SDK.

`AmazonHoneycodeWorkbookFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonHoneycodeWorkbookFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeWorkbookReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Honeycode Workbook über das AWS Management Console und das SDK.

`AmazonHoneycodeWorkbookReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonHoneycodeWorkbookReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2AgentlessServiceRolePolicy

Beschreibung: Gewährt Amazon Inspector Zugriff auf Sicherheitsbewertungen, die für die Durchführung ohne Agenten AWS-Services erforderlich sind

`AmazonInspector2AgentlessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. November 2023, 15:18 Uhr UTC
- Bearbeitete Zeit: 20. November 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2FullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Inspector und Zugriff auf andere verwandte Dienste wie Organisationen.

`AmazonInspector2FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonInspector2FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 19:10 Uhr UTC
- Bearbeitete Zeit: 25. April 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2ManagedCisPolicy

Beschreibung: Dies ist eine verwaltete Richtlinie, die Kunden ihren Rollen zuordnen sollten, um mit dem Inspektor-Service für CIS-Scans zu kommunizieren

`AmazonInspector2ManagedCisPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonInspector2ManagedCisPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Januar 2024, 16:31 UTC
- Bearbeitete Zeit: 24. Januar 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
```

```
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2ReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf den Amazon Inspector2-Service und die entsprechenden Support-Services

`AmazonInspector2ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonInspector2ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Januar 2022, 14:45 UTC
- Bearbeitete Zeit: 22. September 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2ServiceRolePolicy

Beschreibung: Gewährt Amazon Inspector Zugriff auf die für die Durchführung von Sicherheitsbewertungen AWS-Services erforderlichen Daten

`AmazonInspector2ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. November 2021, 20:27 UTC
- Bearbeitete Zeit: 22. Januar 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
```

```
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:ListImages",
        "ecr:PutRegistryScanningConfiguration",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "ssm:DescribeAssociation",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:ListAssociations",
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunction",
        "lambda:GetLayerVersion",
```

```
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GatherInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "DataSyncCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
      ]
    },
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
```

```
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "LambdaCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetAccountConfiguration",
        "codeguru-security:GetFindings",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:DeleteScansByCategory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CodeGuruCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "codeguru-security.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "Ec2DeepInspection",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:GetParameters",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-
paths"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListServiceLinkedChannels",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToRunInvokeCisSpecificDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
      ]
    },
    {
      "Sid" : "AllowToRunCisCommandsToSpecificResources",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToPutCloudwatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Inspector2"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspectorFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Inspector.

`AmazonInspectorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonInspectorFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2015, 17:08 UTC
- Bearbeitete Zeit: 21. Dezember 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspectorReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon Inspector.

`AmazonInspectorReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonInspectorReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2015, 17:08 UTC
- Bearbeitete Zeit: 1. Oktober 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspectorServiceRolePolicy

Beschreibung: Gewährt Amazon Inspector Zugriff auf die für die Durchführung von Sicherheitsbewertungen AWS-Services erforderlichen Daten

`AmazonInspectorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. November 2017, 15:48 Uhr UTC
- Bearbeitete Zeit: 11. September 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKendraFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Kendra über die AWS Management Console.

`AmazonKendraFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKendraFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 16:15 Uhr UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKendraReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Kendra über die AWS Management Console.

`AmazonKendraReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKendraReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 16:13 UTC
- Bearbeitete Zeit: 27. Mai 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKeyspacesFullAccess

Beschreibung: Bieten Sie vollen Zugriff auf Amazon Keyspaces

`AmazonKeyspacesFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKeyspacesFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2020, 17:06 UTC
- Bearbeitete Zeit: 03. Oktober 2023, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ApplicationAutoscalingServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesReplicationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKeyspacesReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon Keyspaces

`AmazonKeyspacesReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKeyspacesReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2020, 17:07 UTC
- Bearbeitete Zeit: 7. Juli 2022, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKeyspacesReadOnlyAccess_v2

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon Keyspaces und verwandte AWS Dienste.

`AmazonKeyspacesReadOnlyAccess_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKeyspacesReadOnlyAccess_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. September 2023, 17:01 UTC
- Bearbeitete Zeit: 12. September 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisAnalyticsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Kinesis Analytics über die AWS Management Console.

`AmazonKinesisAnalyticsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKinesisAnalyticsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. September 2016, 19:01 UTC
- Bearbeitete Zeit: 21. September 2016, 19:01 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisAnalyticsReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Kinesis Analytics über die. AWS Management Console

`AmazonKinesisAnalyticsReadOnly`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKinesisAnalyticsReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. September 2016, 18:16 Uhr UTC
- Bearbeitete Zeit: 21. September 2016, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisFirehoseFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Amazon Kinesis Firehose Delivery Streams.

`AmazonKinesisFirehoseFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKinesisFirehoseFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2015, 18:45 Uhr UTC
- Zeit bearbeitet: 7. Oktober 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisFirehoseReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Amazon Kinesis Firehose Delivery Streams.

`AmazonKinesisFirehoseReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKinesisFirehoseReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2015, 18:43 UTC
- Zeit bearbeitet: 7. Oktober 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Streams über die AWS Management Console.

`AmazonKinesisFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKinesisFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Streams über die AWS Management Console.

`AmazonKinesisReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKinesisReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisVideoStreamsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Kinesis Video Streams über die AWS Management Console.

`AmazonKinesisVideoStreamsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKinesisVideoStreamsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2017, 23:27 UTC
- Zeit bearbeitet: 1. Dezember 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisVideoStreamsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Kinesis Video Streams über die AWS Management Console.

`AmazonKinesisVideoStreamsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonKinesisVideoStreamsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2017, 23:14 Uhr UTC
- Zeit bearbeitet: 1. Dezember 2017, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLaunchWizard_Fullaccess

Beschreibung: Vollzugriff auf den AWS Startassistenten und andere erforderliche Dienste.

`AmazonLaunchWizard_Fullaccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLaunchWizard_Fullaccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. August 2020, 17:47 UTC
- Bearbeitete Zeit: 22. Februar 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLaunchWizardFullAccessV2

Beschreibung: Voller Zugriff auf den AWS Startassistenten und andere erforderliche Dienste.

`AmazonLaunchWizardFullAccessV2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLaunchWizardFullAccessV2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. September 2023, 17:14 Uhr UTC
- Bearbeitete Zeit: 1. September 2023, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexChannelsAccess

Beschreibung: Diese Richtlinie ermöglicht es Kunden, Lex Runtime von Kanälen aus anzurufen

`AmazonLexChannelsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Januar 2021, 20:12 UTC
- Bearbeitete Zeit: 13. Januar 2021, 20:12 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Lex über die AWS Management Console. Bietet außerdem Zugriff zum Erstellen von Lex Service Linked Roles und zum Erteilen von Lex Berechtigungen zum Aufrufen einer begrenzten Anzahl von Lambda-Funktionen.

`AmazonLexFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLexFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. April 2017, 23:20 Uhr UTC
- Bearbeitete Zeit: 16. April 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Lex.

`AmazonLexReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLexReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. April 2017, 23:13 Uhr UTC
- Bearbeitete Zeit: 13. Mai 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexReplicationPolicy

Beschreibung: Ermöglicht Amazon Lex, Lex-Ressourcen in Ihrem Namen regionsübergreifend zu replizieren.

`AmazonLexReplicationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 31. Januar 2024, 23:29 UTC
- Bearbeitete Zeit: 8. März 2024, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex:DeleteBotAlias",
        "lex:DescribeBotAlias",
        "lex:CreateBotVersion",
        "lex:DeleteBotVersion",
        "lex:DescribeBotVersion",
```

```
        "lex:CreateExport",
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",
        "lex:DescribeSlotType",
        "lex:ListSlotTypes",
        "lex:DescribeSlot",
        "lex:ListSlots",
        "lex:DescribeCustomVocabulary",
        "lex:StartImport",
        "lex:DescribeImport",
        "lex:CreateBot",
        "lex:UpdateBot",
        "lex:DeleteBot",
        "lex:CreateBotLocale",
        "lex:UpdateBotLocale",
        "lex:DeleteBotLocale",
        "lex:CreateIntent",
        "lex:UpdateIntent",
        "lex:DeleteIntent",
        "lex:CreateSlotType",
        "lex:UpdateSlotType",
        "lex:DeleteSlotType",
        "lex:CreateSlot",
        "lex:UpdateSlot",
        "lex:DeleteSlot",
        "lex:CreateCustomVocabulary",
        "lex:UpdateCustomVocabulary",
        "lex:DeleteCustomVocabulary",
        "lex:DeleteBotChannel",
        "lex:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:lex:*:*:bot/*",
        "arn:aws:lex:*:*:bot-alias/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "ReplicationServicePolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lex:CreateUploadUrl",
        "lex:ListBots"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lexv2.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexRunBotsOnly

Beschreibung: Bietet Zugriff auf Amazon Lex Conversational APIs.

`AmazonLexRunBotsOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLexRunBotsOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. April 2017, 23:06 UTC
- Bearbeitete Zeit: 18. August 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexV2BotPolicy

Beschreibung: Ermöglicht Lex V2-Bots den Zugriff, um andere AWS Dienste in Ihrem Namen anzurufen.

`AmazonLexV2BotPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Januar 2021, 20:10 UTC
- Bearbeitete Zeit: 13. Januar 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutEquipmentFullAccess

Beschreibung: Bietet vollen Zugriff auf den Betrieb von Amazon Lookout for Equipment

`AmazonLookoutEquipmentFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLookoutEquipmentFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. April 2021, 15:52 UTC
- Bearbeitete Zeit: 24. November 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutEquipmentReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Lookout for Equipments

`AmazonLookoutEquipmentReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLookoutEquipmentReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 05. Mai 2021, 16:47 UTC
- Bearbeitete Zeit: 10. November 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutMetricsFullAccess

Beschreibung: Ermöglicht den Zugriff auf alle Aktionen für Amazon Lookout for Metrics

`AmazonLookoutMetricsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLookoutMetricsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Mai 2021, 00:43 UTC
- Bearbeitete Zeit: 7. Mai 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutMetricsReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf alle schreibgeschützten Aktionen für Amazon Lookout for Metrics

`AmazonLookoutMetricsReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLookoutMetricsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Mai 2021, 00:43 UTC
- Bearbeitete Zeit: 4. Januar 2022, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutVisionConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Lookout for Vision und bereichsspezifischen Zugriff auf erforderliche Service- und Konsolenabhängigkeiten.

`AmazonLookoutVisionConsoleFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLookoutVisionConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2021, 19:37 UTC
- Bearbeitete Zeit: 11. Mai 2021, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutVisionConsoleReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon Lookout for Vision und bereichsspezifischen Zugriff auf erforderliche Service- und Konsolenabhängigkeiten.

`AmazonLookoutVisionConsoleReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLookoutVisionConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 11. Mai 2021, 19:32 UTC
- Bearbeitete Zeit: 9. Dezember 2021, 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutVisionFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Lookout for Vision und bereichsspezifischen Zugriff auf erforderliche Abhängigkeiten.

`AmazonLookoutVisionFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLookoutVisionFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2021, 19:24 UTC
- Bearbeitete Zeit: 11. Mai 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutVisionReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon Lookout for Vision und bereichsspezifischen Zugriff auf erforderliche Abhängigkeiten.

`AmazonLookoutVisionReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonLookoutVisionReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2021, 19:11 UTC
- Bearbeitete Zeit: 9. Dezember 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningBatchPredictionsAccess

Beschreibung: Erteilt Benutzern die Erlaubnis, Amazon Machine Learning Learning-Batchvorhersagen anzufordern.

`AmazonMachineLearningBatchPredictionsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMachineLearningBatchPredictionsAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:12 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningCreateOnlyAccess

Beschreibung: Bietet Erstellungszugriff für Amazon Machine Learning Learning-Ressourcen ohne Vorhersage.

`AmazonMachineLearningCreateOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMachineLearningCreateOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:18 Uhr UTC
- Bearbeitete Zeit: 29. Juni 2016, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Machine Learning Learning-Ressourcen.

`AmazonMachineLearningFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMachineLearningFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:25 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Beschreibung: Erteilt Benutzern die Erlaubnis, den Echtzeit-Endpunkt für Amazon Machine Learning Learning-Modelle zu erstellen und zu löschen.

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMachineLearningManageRealTimeEndpointOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:32 UTC
- Zeit bearbeitet: 9. April 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "machinelearning:CreateRealtimeEndpoint",
        "machinelearning:DeleteRealtimeEndpoint"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon Machine Learning Learning-Ressourcen.

`AmazonMachineLearningReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMachineLearningReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:40 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningRealTimePredictionOnlyAccess

Beschreibung: Erteilt Benutzern die Erlaubnis, Echtzeitvorhersagen von Amazon Machine Learning anzufordern.

`AmazonMachineLearningRealTimePredictionOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMachineLearningRealTimePredictionOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:44 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningRoleforRedshiftDataSourceV3

Beschreibung: Ermöglicht Machine Learning, Ihre Redshift-Cluster und S3-Staging-Standorte für die Redshift-Datenquelle zu konfigurieren und zu verwenden.

`AmazonMachineLearningRoleforRedshiftDataSourceV3`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMachineLearningRoleforRedshiftDataSourceV3` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. Juni 2020, 18:00 Uhr UTC
- Bearbeitete Zeit: 24. Juni 2020, 18:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Macie.

`AmazonMacieFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMacieFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. August 2017, 14:54 UTC
- Bearbeitete Zeit: 1. Juli 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieHandshakeRole

Beschreibung: Erteilt die Erlaubnis, die servicebezogene Rolle von Amazon Macie zu erstellen.

`AmazonMacieHandshakeRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMacieHandshakeRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 28. Juni 2018, 15:46 Uhr UTC
- Bearbeitete Zeit: 28. Juni 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Macie.

`AmazonMacieReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMacieReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Juni 2023, 21:50 UTC
- Bearbeitete Zeit: 15. Juni 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieServiceRole

Beschreibung: Gewährt Macie nur Lesezugriff auf Ressourcenabhängigkeiten in Ihrem Konto, um die Datenanalyse zu ermöglichen.

`AmazonMacieServiceRole`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMacieServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 14:53 Uhr UTC
- Zeit bearbeitet: 14. August 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieServiceRolePolicy

Beschreibung: Serviceverknüpfte Rolle für Amazon Macie

`AmazonMacieServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Juni 2018, 22:17 UTC
- Bearbeitete Zeit: 19. Mai 2022, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonManagedBlockchainConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Managed Blockchain über AWS Management Console

`AmazonManagedBlockchainConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonManagedBlockchainConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. April 2019, 21:23 Uhr UTC
- Bearbeitete Zeit: 29. April 2019, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonManagedBlockchainFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Managed Blockchain.

`AmazonManagedBlockchainFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonManagedBlockchainFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 29. April 2019, 21:39 Uhr UTC
- Bearbeitete Zeit: 29. April 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonManagedBlockchainReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Managed Blockchain.

`AmazonManagedBlockchainReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonManagedBlockchainReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. April 2019, 18:17 UTC
- Bearbeitete Zeit: 30. April 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonManagedBlockchainServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon Managed Blockchain verwendet oder verwaltet werden

`AmazonManagedBlockchainServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Januar 2020, 19:51 UTC
- Zeit bearbeitet: 17. Januar 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMCSFullAccess

Beschreibung: Bieten Sie vollen Zugriff auf Amazon Managed Apache Cassandra Service

`AmazonMCSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMCSFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 13:45 Uhr UTC
- Bearbeitete Zeit: 17. April 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMCSReadOnlyAccess

Beschreibung: Bieten Sie nur Lesezugriff auf Amazon Managed Apache Cassandra Service

`AmazonMCSReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMCSReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 13:46 UTC
- Bearbeitete Zeit: 17. April 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMechanicalTurkFullAccess

Beschreibung: Bietet vollen Zugriff auf alle APIs in Amazon Mechanical Turk.

`AmazonMechanicalTurkFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMechanicalTurkFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2015, 19:08 Uhr UTC
- Bearbeitete Zeit: 11. Dezember 2015, 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMechanicalTurkReadOnly

Beschreibung: Bietet Zugriff auf schreibgeschützte APIs in Amazon Mechanical Turk.

`AmazonMechanicalTurkReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMechanicalTurkReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2015, 19:08 Uhr UTC
- Bearbeitete Zeit: 25. September 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMemoryDBFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon MemoryDB über die. AWS Management Console

`AmazonMemoryDBFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMemoryDBFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Oktober 2021, 19:24 UTC
- Bearbeitete Zeit: 8. Oktober 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMemoryDBReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon MemoryDB über die. AWS Management Console

`AmazonMemoryDBReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMemoryDBReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Oktober 2021, 19:27 UTC
- Bearbeitete Zeit: 8. Oktober 2021, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMobileAnalyticsFinancialReportAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Berichte, einschließlich Finanzdaten für alle Anwendungsressourcen.

`AmazonMobileAnalyticsFinancialReportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMobileAnalyticsFinancialReportAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMobileAnalyticsFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Anwendungsressourcen.

`AmazonMobileAnalyticsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMobileAnalyticsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC

- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMobileAnalyticsNon-financialReportAccess

Beschreibung: Bietet Lesezugriff auf Berichte, die keine Finanzberichte sind, für alle Anwendungsressourcen.

`AmazonMobileAnalyticsNon-financialReportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMobileAnalyticsNon-financialReportAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMobileAnalyticsWriteOnlyAccess

Beschreibung: Bietet nur Schreibzugriff auf Put-Ereignisdaten für alle Anwendungsressourcen. (Für die SDK-Integration empfohlen)

`AmazonMobileAnalyticsWriteOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMobileAnalyticsWriteOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMonitronFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung von Amazon Monitron

`AmazonMonitronFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMonitronFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Dezember 2020, 22:40 UTC
- Bearbeitete Zeit: 8. Juni 2022, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQApiFullAccess

Beschreibung: Bietet vollen Zugriff auf AmazonMQ über unsere API/SDK.

`AmazonMQApiFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMQApiFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Dezember 2018, 20:31 UTC
- Bearbeitete Zeit: 4. November 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQApiReadOnlyAccess

Beschreibung: Bietet über unsere API/SDK nur Lesezugriff auf AmazonMQ.

`AmazonMQApiReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMQApiReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Dezember 2018, 20:31 UTC
- Bearbeitete Zeit: 18. Dezember 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQFullAccess

Beschreibung: Bietet vollen Zugriff auf AmazonMQ über die. AWS Management Console

`AmazonMQFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMQFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2017, 15:28 Uhr UTC
- Zeit bearbeitet: 4. November 2020, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AmazonMQ über die. AWS Management Console

`AmazonMQReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMQReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2017, 15:30 Uhr UTC
- Bearbeitete Zeit: 28. November 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQServiceRolePolicy

Beschreibung: Richtlinie für serviceverknüpfte Rollen für AWS Amazon MQ

`AmazonMQServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. November 2020, 16:07 UTC
- Bearbeitete Zeit: 4. November 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMSKConnectReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon MSK Connect

`AmazonMSKConnectReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMSKConnectReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. September 2021, 10:18 Uhr UTC
- Bearbeitete Zeit: 18. Oktober 2021, 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMSKFullAccess

Beschreibung: Gewähren Sie vollen Zugriff auf Amazon MSK und andere erforderliche Berechtigungen für dessen Abhängigkeiten.

`AmazonMSKFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMSKFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Januar 2019, 22:07 UTC
- Bearbeitete Zeit: 18. Oktober 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMSKReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon MSK

`AmazonMSKReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonMSKReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Januar 2019, 22:28 UTC
- Bearbeitete Zeit: 14. Januar 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMWAAServiceRolePolicy

Beschreibung: Die serviceverknüpfte Rolle, die von Amazon Managed Workflows für Apache Airflow verwendet wird.

`AmazonMWAAServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. November 2020, 14:13 Uhr UTC
- Zeit bearbeitet: 17. November 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonNimbleStudio-LaunchProfileWorker

Beschreibung: Diese Richtlinie gewährt Zugriff auf Ressourcen, die von Nimble Studio Launch Profile-Workern benötigt werden. Hängen Sie diese Richtlinie an EC2-Instances an, die von Nimble Studio Builder erstellt wurden.

`AmazonNimbleStudio-LaunchProfileWorker`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonNimbleStudio-LaunchProfileWorker` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. April 2021, 04:47 UTC
- Bearbeitete Zeit: 28. April 2021, 04:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonNimbleStudio-StudioAdmin

Beschreibung: Diese Richtlinie gewährt Zugriff auf Amazon Nimble Studio-Ressourcen, die mit dem Studio-Administrator verknüpft sind, und auf zugehörige Studio-Ressourcen in anderen Diensten. Fügen Sie diese Richtlinie der Administratorrolle hinzu, die Ihrem Studio zugeordnet ist.

`AmazonNimbleStudio-StudioAdmin`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonNimbleStudio-StudioAdmin` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. April 2021, 04:47 UTC
- Bearbeitete Zeit: 22. September 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonNimbleStudio-StudioUser

Beschreibung: Diese Richtlinie gewährt Zugriff auf Amazon Nimble Studio-Ressourcen, die mit dem Studio-Benutzer verknüpft sind, und auf zugehörige Studio-Ressourcen in anderen Diensten. Fügen Sie diese Richtlinie der Benutzerrolle hinzu, die Ihrem Studio zugeordnet ist.

`AmazonNimbleStudio-StudioUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonNimbleStudio-StudioUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. April 2021, 04:48 UTC
- Bearbeitete Zeit: 22. September 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOmicsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Omics und andere erforderliche AWS-Services Funktionen. Diese Richtlinie ermöglicht es dem Benutzer, RAM-Share-Einladungen einzusehen und anzunehmen, um auf Ressourcen zuzugreifen, die sich nicht auf die des Benutzers AWS-Konto beziehen.

`AmazonOmicsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOmicsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Februar 2023, 00:59 UTC
- Bearbeitete Zeit: 24. Februar 2023, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOmicsReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon Omics

`AmazonOmicsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOmicsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2022, 04:17 UTC
- Bearbeitete Zeit: 29. November 2022, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOneEnterpriseFullAccess

Beschreibung: Diese Richtlinie gewährt Administratorberechtigungen, die den Zugriff auf alle Ressourcen und Abläufe von Amazon One Enterprise ermöglichen.

`AmazonOneEnterpriseFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOneEnterpriseFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 04:58 UTC
- Bearbeitete Zeit: 28. November 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Sid" : "FullAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOneEnterpriseInstallerAccess

Beschreibung: Diese Richtlinie gewährt eingeschränkte Lese- und Schreibberechtigungen, die die Installation und Aktivierung von Geräten ermöglichen.

`AmazonOneEnterpriseInstallerAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOneEnterpriseInstallerAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 05:00 UTC
- Bearbeitete Zeit: 28. November 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOneEnterpriseReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt allen Amazon One Enterprise-Ressourcen und -Vorgängen nur Leseberechtigungen.

`AmazonOneEnterpriseReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOneEnterpriseReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 04:59 UTC
- Bearbeitete Zeit: 28. November 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "one:Get*",
        "one:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchDashboardsServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf Amazon OpenSearch Dashboards Service, um auf andere AWS Dienste zuzugreifen, z. B. in CloudWatch Ihrem Namen

`AmazonOpenSearchDashboardsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. Dezember 2023, 19:38 UTC
- Bearbeitete Zeit: 22. Dezember 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchDirectQueryGlueCreateAccess

Beschreibung: Ermöglicht dem OpenSearch DirectQuery Service den Zugriff auf AWS Glue-APIs, um Ressourcen in Ihrem Namen zu erstellen.

`AmazonOpenSearchDirectQueryGlueCreateAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOpenSearchDirectQueryGlueCreateAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Mai 2024, 12:24 UTC
- Bearbeitungszeit: 6. Mai 2024, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchIngestionFullAccess

Beschreibung: Ermöglicht Amazon OpenSearch Ingestion, in Ihrem Namen auf andere AWS Dienste zuzugreifen.

`AmazonOpenSearchIngestionFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOpenSearchIngestionFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. April 2023, 18:11 UTC
- Bearbeitete Zeit: 26. April 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchIngestionReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Amazon OpenSearch Ingestion Service

`AmazonOpenSearchIngestionReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOpenSearchIngestionReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. April 2023, 18:09 UTC
- Bearbeitete Zeit: 26. April 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchIngestionServiceRolePolicy

Beschreibung: Ermöglicht Amazon OpenSearch Ingestion Service, in Ihrem Namen auf andere AWS Dienste zuzugreifen.

`AmazonOpenSearchIngestionServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2022, 16:49 UTC

- Bearbeitete Zeit: 18. November 2022, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServerlessServiceRolePolicy

Beschreibung: Erlauben Sie Amazon OpenSearch Serverless, in Ihrem Namen auf andere AWS Dienste wie CloudWatch APIs zuzugreifen.

`AmazonOpenSearchServerlessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. November 2022, 19:50 UTC
- Bearbeitete Zeit: 24. November 2022, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServiceCognitoAccess

Beschreibung: Ermöglicht den Zugriff auf den Amazon Cognito Cognito-Konfigurationsservice.

`AmazonOpenSearchServiceCognitoAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOpenSearchServiceCognitoAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. September 2021, 06:31 UTC
- Bearbeitete Zeit: 20. Dezember 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServiceFullAccess

Beschreibung: Bietet vollen Zugriff auf den Amazon OpenSearch Service-Konfigurationsservice.

`AmazonOpenSearchServiceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOpenSearchServiceFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 08. September 2021, 05:33 UTC
- Bearbeitete Zeit: 8. September 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServiceReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Amazon OpenSearch Service-Konfigurationsservice.

`AmazonOpenSearchServiceReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonOpenSearchServiceReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 08. September 2021, 05:38 UTC
- Bearbeitete Zeit: 8. September 2021, 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServiceRolePolicy

Beschreibung: Erlauben Sie Amazon OpenSearch Service, in Ihrem Namen auf andere AWS Dienste wie EC2 Networking APIs zuzugreifen.

`AmazonOpenSearchServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. August 2021, 09:27 UTC
- Bearbeitete Zeit: 23. Oktober 2023, 07:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973154",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973164",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973174",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973184",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973195",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973196",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973197",
      "Effect" : "Allow",
```

```
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPersonalizeFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Personalize über das AWS Management Console und SDK. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, CloudWatch).

`AmazonPersonalizeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonPersonalizeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. Dezember 2018, 22:24 Uhr UTC
- Bearbeitete Zeit: 30. Mai 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPollyFullAccess

Beschreibung: Gewährt vollen Zugriff auf den Service und die Ressourcen von Amazon Polly.

`AmazonPollyFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonPollyFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 18:59 Uhr UTC
- Bearbeitete Zeit: 30. November 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPollyReadOnlyAccess

Beschreibung: Gewährt schreibgeschützten Zugriff auf Amazon Polly Polly-Ressourcen.

`AmazonPollyReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonPollyReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 18:59 Uhr UTC
- Bearbeitete Zeit: 17. Juli 2018, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusConsoleFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS verwaltete Prometheus-Ressourcen in der Konsole AWS

`AmazonPrometheusConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonPrometheusConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 18:11 Uhr UTC
- Zeit bearbeitet: 24. Oktober 2022, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
```

```
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
        "aps:DeleteWorkspace",
        "aps:ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:CreateAlertManagerDefinition",
        "aps:CreateRuleGroupsNamespace",
        "aps:DeleteAlertManagerDefinition",
        "aps:DeleteRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DeleteLoggingConfiguration",
        "aps:DescribeLoggingConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS verwaltete Prometheus-Ressourcen

`AmazonPrometheusFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonPrometheusFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 18:10 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusQueryAccess

Beschreibung: Gewährt Zugriff zum Ausführen von Abfragen für AWS verwaltete Prometheus-Ressourcen

`AmazonPrometheusQueryAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonPrometheusQueryAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Dezember 2020, 01:02 UTC
- Bearbeitete Zeit: 19. Dezember 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusRemoteWriteAccess

Beschreibung: Gewährt nur Schreibzugriff auf AWS verwaltete Prometheus-Arbeitsbereiche

`AmazonPrometheusRemoteWriteAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonPrometheusRemoteWriteAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Dezember 2020, 01:04 UTC
- Bearbeitete Zeit: 19. Dezember 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusScraperServiceRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von Amazon Managed Service für Prometheus Collector verwaltet oder verwendet werden

`AmazonPrometheusScraperServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 26. November 2023, 14:19 UTC
- Bearbeitete Zeit: 26. April 2024, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQFullAccess

Beschreibung: Bietet vollen Zugriff, um Interaktionen mit Amazon Q zu ermöglichen

`AmazonQFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonQFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 16:00 Uhr UTC
- Bearbeitete Zeit: 29. April 2024, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
```

```
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQLDBConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon QLDB über die. AWS Management Console

`AmazonQLDBConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonQLDBConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. September 2019, 18:24 Uhr UTC
- Bearbeitete Zeit: 4. November 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQLDBFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon QLDB über die Service-API.

`AmazonQLDBFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonQLDBFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. September 2019, 18:23 Uhr UTC
- Bearbeitete Zeit: 4. November 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQLDBReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon QLDB.

`AmazonQLDBReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonQLDBReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. September 2019, 18:19 Uhr UTC
- Bearbeitete Zeit: 2. Juli 2021, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSBetaServiceRolePolicy

Beschreibung: Ermöglicht Amazon RDS, AWS Ressourcen in Ihrem Namen zu verwalten.

`AmazonRDSBetaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Mai 2018, 19:41 UTC
- Bearbeitete Zeit: 14. Dezember 2022, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
```

```
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
```

```
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSCustomInstanceProfileRolePolicy

Beschreibung: Ermöglicht Amazon RDS Custom, verschiedene Automatisierungsaktionen und Datenbankverwaltungsaufgaben über ein EC2-Instance-Profil auszuführen.

`AmazonRDSCustomInstanceProfileRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRDSCustomInstanceProfileRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Februar 2024, 17:42 UTC
- Bearbeitete Zeit: 27. Februar 2024, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssmAgentPermission4",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission5",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "createEc2SnapshotPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission3",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createTagForEc2SnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "rdsCustomS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "rdsCustomS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "readSecretsFromCpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "createSecretsOnDpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "publishCwMetricsPermission",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "rdscustom/rds-custom-sqlserver-agent",
            "RDSCustomForOracle/Agent"
          ]
        }
      }
    },
    {
      "Sid" : "putEventsToEventBusPermission",
      "Effect" : "Allow",
      "Action" : "events:PutEvents",
      "Resource" : "arn:aws:events:*:*:event-bus/default"
    },
    {
      "Sid" : "cwlUploadPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutRetentionPolicy",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
```

```
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
    },
    {
      "Sid" : "sendMessageToSqsQueuePermission",
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
        }
      }
    },
    {
      "Sid" : "managePrivateIpOnEniPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithSecret",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:do-
not-delete-rds-custom-*"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithS3",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-rds-custom-
*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSCustomPreviewServiceRolePolicy

Beschreibung: Rollenrichtlinie für Amazon RDS Custom Preview Service

`AmazonRDSCustomPreviewServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Oktober 2021, 21:44 UTC
- Bearbeitete Zeit: 20. September 2023, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "eccVolume2",
    "Effect" : "Allow",
    "Action" : "ec2:CreateVolume",
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "StringLike" : {
        "aws:RequestTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccVolume3",
    "Effect" : "Allow",
    "Action" : [
      "ec2:ModifyVolumeAttribute",
      "ec2:DeleteVolume",
      "ec2:ModifyVolume"
    ],
    "Resource" : "arn:aws:ec2:*:*:volume/*",
    "Condition" : {
      "StringLike" : {
        "aws:ResourceTag/AWSRDSCustom" : [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    }
  },
  {
    "Sid" : "eccVolume4snapshot1",
    "Effect" : "Allow",
    "Action" : [
      "ec2:CreateVolume",
      "ec2:DeleteSnapshot"
```

```
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
```

```
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
```

```
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSCustomServiceRolePolicy

Beschreibung: Ermöglicht Amazon RDS Custom, AWS Ressourcen in Ihrem Namen zu verwalten.

`AmazonRDSCustomServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Oktober 2021, 21:39 UTC
- Bearbeitete Zeit: 19. April 2024, 15:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "eccModifyInstanceAttribute1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ],
          "ec2:Attribute" : "InstanceType"
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag2",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshot",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "eccSnapshot4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSRDSCustom*",
        "arn:aws:iam::*:role/service-role/AWSRDSCustom*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
```

```
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSDataFullAccess

Beschreibung: Ermöglicht vollen Zugriff auf die Verwendung der RDS-Daten-APIs, Secret Store-APIs für RDS-Datenbankanmeldedaten und der DB-Konsolen-Abfrageverwaltungs-APIs zur Ausführung von SQL-Anweisungen auf Aurora Serverless-Clustern in der AWS-Konto.

`AmazonRDSDataFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRDSDataFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2018, 21:29 Uhr UTC
- Bearbeitete Zeit: 20. November 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSDirectoryServiceAccess

Beschreibung: Erlauben Sie RDS, im Namen des Kunden auf Directory Service Managed AD für domänengebundene SQL Server-DB-Instances zuzugreifen.

`AmazonRDSDirectoryServiceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRDSDirectoryServiceAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Februar 2016, 02:02 UTC
- Bearbeitete Zeit: 15. Mai 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSEnhancedMonitoringRole

Beschreibung: Bietet Zugriff auf Cloudwatch for RDS Enhanced Monitoring

`AmazonRDSEnhancedMonitoringRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRDSEnhancedMonitoringRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. November 2015, 19:58 Uhr UTC
- Zeit bearbeitet: 11. November 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon RDS über die AWS Management Console.

`AmazonRDSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRDSFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 17. August 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSPerformanceInsightsFullAccess

Beschreibung: Bietet vollen Zugriff auf RDS Performance Insights über AWS Management Console

`AmazonRDSPerformanceInsightsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRDSPerformanceInsightsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. August 2023, 23:41 UTC
- Bearbeitete Zeit: 23. Oktober 2023, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
```

```
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReports",
        "pi:DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    },
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSPerformanceInsightsReadOnly

Beschreibung: Nur-Lese-Richtlinie für RDS Performance Insights

`AmazonRDSPerformanceInsightsReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRDSPerformanceInsightsReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. April 2022, 00:02 UTC
- Bearbeitete Zeit: 23. Oktober 2023, 21:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
      "Action" : "pi:DescribeDimensionKeys",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
      "Effect" : "Allow",
      "Action" : "pi:GetDimensionKeyDetails",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetadata",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
```

```
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceDimensions",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
      "Effect" : "Allow",
      "Action" : "pi:GetPerformanceAnalysisReport",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReports",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
      "Effect" : "Allow",
      "Action" : "pi:ListTagsForResource",
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSPreviewServiceRolePolicy

Beschreibung: Rollenrichtlinie für Amazon RDS Preview Service

`AmazonRDSPreviewServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 31. Mai 2018, 18:02 Uhr UTC
- Bearbeitete Zeit: 4. Oktober 2023, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Preview",
            "AWS/Neptune-Preview",
            "AWS/RDS-Preview",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon RDS über die AWS Management Console.

`AmazonRDSReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRDSReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 14. April 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSServiceRolePolicy

Beschreibung: Ermöglicht Amazon RDS, AWS Ressourcen in Ihrem Namen zu verwalten.

`AmazonRDSServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Januar 2018, 18:17 UTC
- Bearbeitete Zeit: 19. Januar 2024, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossRegionCommunication",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
```

```
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Sns",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ]
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*",
```

```
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "Kinesis",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream",
        "kinesis:SplitShard",
        "kinesis:MergeShards",
        "kinesis:DeleteStream",
        "kinesis:UpdateShardCount"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
      ]
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    },
    {
      "Sid" : "SecretsManagerTags",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftAllCommandsFullAccess

Beschreibung: Diese Richtlinie umfasst Berechtigungen zur Ausführung von SQL-Befehlen zum Kopieren, Laden, Entladen, Abfragen und Analysieren von Daten auf Amazon Redshift. Die Richtlinie gewährt auch Berechtigungen zur Ausführung ausgewählter Anweisungen für verwandte Dienste wie Amazon S3, Amazon CloudWatch Logs SageMaker, Amazon oder AWS Glue.

`AmazonRedshiftAllCommandsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRedshiftAllCommandsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. November 2021, 00:48 UTC
- Bearbeitete Zeit: 25. November 2021, 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftDataFullAccess

Beschreibung: Diese Richtlinie bietet vollen Zugriff auf Amazon Redshift Data APIs. Diese Richtlinie gewährt auch bereichsbezogenen Zugriff auf andere erforderliche Dienste.

`AmazonRedshiftDataFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRedshiftDataFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. September 2020, 19:23 UTC
- Bearbeitete Zeit: 7. April 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Redshift über die AWS Management Console.

`AmazonRedshiftFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRedshiftFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 7. Juli 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditor

Beschreibung: Bietet vollen Zugriff auf den Amazon Redshift Query Editor und auf gespeicherte Abfragen über die AWS Management Console.

`AmazonRedshiftQueryEditor`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRedshiftQueryEditor` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Oktober 2018, 22:50 UTC
- Bearbeitete Zeit: 16. Februar 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditorV2FullAccess

Beschreibung: Gewährt vollen Zugriff auf die Vorgänge und Ressourcen des Amazon Redshift Query Editor V2. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon Redshift Redshift-Cluster, zum Lesen von Schlüsseln und Aliasen in AWS KMS und zum Verwalten der Query Editor V2-Geheimnisse in AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRedshiftQueryEditorV2FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:06 UTC
- Bearbeitete Zeit: 21. Februar 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditorV2NoSharing

Beschreibung: Ermöglicht die Arbeit mit Amazon Redshift Query Editor V2, ohne Ressourcen gemeinsam zu nutzen. Der bewilligte Principal kann nur seine eigenen Ressourcen lesen, aktualisieren und löschen, sie jedoch nicht gemeinsam nutzen. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon Redshift Redshift-Cluster und zum Verwalten der Query Editor V2-Geheimnisse des Prinzipals in AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2NoSharing`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRedshiftQueryEditorV2NoSharing` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:18 Uhr UTC
- Bearbeitete Zeit: 21. Februar 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditorV2ReadSharing

Beschreibung: Ermöglicht die Arbeit mit Amazon Redshift Query Editor V2 mit begrenzter gemeinsamer Nutzung von Ressourcen. Der bewilligte Principal kann seine eigenen Ressourcen lesen, schreiben und gemeinsam nutzen. Der erteilte Prinzipal kann die mit seinem Team gemeinsam genutzten Ressourcen lesen, sie jedoch nicht aktualisieren. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon Redshift Redshift-Cluster und zum Verwalten der Query Editor V2-Geheimnisse des Prinzipals in AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadSharing`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRedshiftQueryEditorV2ReadSharing` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:22 Uhr UTC
- Bearbeitete Zeit: 21. Februar 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditorV2ReadWriteSharing

Beschreibung: Ermöglicht die Arbeit mit Amazon Redshift Query Editor V2 mit gemeinsamer Nutzung von Ressourcen. Der bewilligte Principal kann seine eigenen Ressourcen lesen, schreiben und gemeinsam nutzen. Der Prinzipal mit den entsprechenden Berechtigungen kann die mit seinem Team geteilten Ressourcen lesen und bearbeiten. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon Redshift Redshift-Cluster und zum Verwalten der Query Editor V2-Geheimnisse des Prinzipals in AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadWriteSharing`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRedshiftQueryEditorV2ReadWriteSharing` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:25 Uhr UTC
- Bearbeitete Zeit: 21. Februar 2024, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Redshift über die AWS Management Console.

`AmazonRedshiftReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRedshiftReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 8. Februar 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Redshift, AWS Dienste in Ihrem Namen anzurufen

`AmazonRedshiftServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. September 2017, 19:19 Uhr UTC
- Bearbeitete Zeit: 15. März 2024, 20:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRekognitionCustomLabelsFullAccess

Beschreibung: Diese Richtlinie spezifiziert Rekognition- und S3-Berechtigungen, die für die Amazon Rekognition Custom Labels-Funktion erforderlich sind.

`AmazonRekognitionCustomLabelsFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRekognitionCustomLabelsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Januar 2020, 19:18 UTC
- Zeit bearbeitet: 16. August 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRekognitionFullAccess

Beschreibung: Zugriff auf alle Amazon Rekognition APIs

`AmazonRekognitionFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRekognitionFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 14:40 Uhr UTC
- Bearbeitete Zeit: 30. November 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRekognitionReadOnlyAccess

Beschreibung: Zugriff auf alle Read Rekognition APIs

`AmazonRekognitionReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRekognitionReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 14:58 Uhr UTC
- Bearbeitete Zeit: 8. November 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRekognitionServiceRole

Beschreibung: Ermöglicht Rekognition, AWS Dienste in Ihrem Namen anzurufen.

`AmazonRekognitionServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRekognitionServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. November 2017, 16:52 UTC
- Zeit bearbeitet: 29. November 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53AutoNamingFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Route 53 53-Aktionen zur automatischen Benennung.

`AmazonRoute53AutoNamingFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53AutoNamingFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2018, 18:40 Uhr UTC
- Bearbeitete Zeit: 18. Januar 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53AutoNamingReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Route 53 53-Aktionen zur automatischen Benennung.

`AmazonRoute53AutoNamingReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53AutoNamingReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2018, 03:02 UTC
- Bearbeitete Zeit: 18. Januar 2018, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53AutoNamingRegistrantAccess

Beschreibung: Bietet Zugriff auf Registrantenebene auf Route 53 53-Aktionen zur automatischen Benennung.

`AmazonRoute53AutoNamingRegistrantAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53AutoNamingRegistrantAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. März 2018, 22:33 UTC
- Bearbeitete Zeit: 12. März 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53DomainsFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Route53-Domänen-Aktionen und ermöglicht die Erstellung von Hosting-Zonen im Rahmen von Domainregistrierungen.

`AmazonRoute53DomainsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53DomainsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53DomainsReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf die Liste und die Aktionen der Route53-Domänen.

`AmazonRoute53DomainsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53DomainsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53FullAccess

Beschreibung: Bietet vollen Zugriff auf alle Amazon Route 53 über die AWS Management Console.

`AmazonRoute53FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 20. Dezember 2018, 21:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ProfilesFullAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf Amazon Route 53 53-Profilressourcen.

`AmazonRoute53ProfilesFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53ProfilesFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 30. April 2024, 18:30 Uhr UTC
- Bearbeitete Zeit: 30. April 2024, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:CreateProfile",
        "route53profiles:DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
```

```
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ProfilesReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Lesezugriff auf Amazon Route 53 53-Profilressourcen.

`AmazonRoute53ProfilesReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53ProfilesReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. April 2024, 18:29 UTC
- Bearbeitete Zeit: 30. April 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Amazon Route 53 über die AWS Management Console.

`AmazonRoute53ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 15. November 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryClusterFullAccess

Beschreibung: Bietet vollen Zugriff auf den Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53RecoveryClusterFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 18:37 UTC
- Bearbeitete Zeit: 18. August 2021, 18:37 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryClusterReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53RecoveryClusterReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 17:36 Uhr UTC
- Bearbeitete Zeit: 1. April 2022, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryControlConfigFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53RecoveryControlConfigFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 17:48 Uhr UTC
- Bearbeitete Zeit: 18. August 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53RecoveryControlConfigReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 18:01 UTC

- Bearbeitete Zeit: 18. Oktober 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryReadinessFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53RecoveryReadinessFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 16:45 Uhr UTC
- Bearbeitete Zeit: 18. August 2021, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryReadinessReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53RecoveryReadinessReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 18:11 Uhr UTC

- Zeit bearbeitet: 09. November 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ResolverFullAccess

Beschreibung: Vollständige Zugriffsrichtlinie für Route 53 Resolver

`AmazonRoute53ResolverFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53ResolverFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2019, 18:10 Uhr UTC
- Bearbeitete Zeit: 17. Juli 2020, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ResolverReadOnlyAccess

Beschreibung: Schreibgeschützte Richtlinie für Route 53 Resolver

`AmazonRoute53ResolverReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonRoute53ResolverReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2019, 18:11 Uhr UTC
- Bearbeitete Zeit: 27. September 2019, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3FullAccess

Beschreibung: Bietet vollen Zugriff auf alle Buckets über die AWS Management Console.

`AmazonS3FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonS3FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 27. September 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3ObjectLambdaExecutionRolePolicy

Beschreibung: Stellt AWS Lambda-Funktionen Berechtigungen für die Interaktion mit Amazon S3 Object Lambda bereit. Gewährt Lambda außerdem Berechtigungen zum Schreiben in CloudWatch Logs.

`AmazonS3ObjectLambdaExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonS3ObjectLambdaExecutionRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 18. August 2021, 10:07 UTC
- Bearbeitete Zeit: 18. August 2021, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3OutpostsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon S3 auf Outposts über die AWS Management Console.

`AmazonS3OutpostsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonS3OutpostsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Oktober 2020, 17:26 UTC
- Bearbeitete Zeit: 2. Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3OutpostsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon S3 auf Outposts über die AWS Management Console.

`AmazonS3OutpostsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonS3OutpostsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Oktober 2020, 18:55 UTC
- Bearbeitete Zeit: 2. Oktober 2020, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Buckets über die AWS Management Console.

`AmazonS3ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonS3ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 10. August 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Beschreibung: Servicerollenrichtlinie, die vom AWS-Service Catalog Service verwendet wird, um Produkte aus dem SageMaker Amazon-Produktportfolio bereitzustellen. Gewährt Berechtigungen für eine Reihe verwandter Dienste CodePipeline CodeBuild CodeCommit, darunter, CloudFormation, Glue usw.

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2020, 18:48 Uhr UTC
- Bearbeitete Zeit: 12. Juni 2024, 18:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PATCH"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "ArnLikeIfExists" : {
          "cloudformation:RoleArn" : [
            "arn:aws:sts::*:assumed-role/AmazonSageMakerServiceCatalog*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateCommit",
        "codecommit:CreateRepository",
        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
      ],
      "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateUserPool",
        "cognito-idp:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
```

```
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
```

```
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateClassifier",
        "glue:DeleteClassifier",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeleteTrigger",
        "glue:DeleteWorkflow",
        "glue:StopCrawler"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateWorkflow"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:CreateJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:GetCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
```

```
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
        "arn:aws:logs:*:*:log-group::log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
      ],
      "Resource" : "arn:aws:s3:::sagemaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
```

```
        "sagemaker:CreateCodeRepository",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:DeleteCodeRepository"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateImage",
        "sagemaker:DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "states:CreateStateMachine",
        "states:DeleteStateMachine",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*",
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasAIServicesAccess

Beschreibung: Ermöglicht Amazon SageMaker Canvas die Nutzung von KI-Services zur Unterstützung einsatzbereiter KI-Lösungen. Diese Richtlinie wird weitere Mutationsberechtigungen für Dienste hinzufügen, sobald Amazon SageMaker Canvas Unterstützung anbietet.

`AmazonSageMakerCanvasAIServicesAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerCanvasAIServicesAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. März 2023, 22:36 UTC
- Bearbeitete Zeit: 29. November 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasBedrockAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen zur Nutzung von Amazon Bedrock in SageMaker Canvas, indem sie Zugriff auf nachgelagerte Dienste wie S3 gewährt.

`AmazonSageMakerCanvasBedrockAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerCanvasBedrockAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. Februar 2024, 18:37 UTC
- Bearbeitete Zeit: 2. Februar 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasDataPrepFullAccess

Beschreibung: Bietet vollen Zugriff auf SageMaker Amazon-Ressourcen und -Operationen für die Datenaufbereitung in Canvas. Die Richtlinie bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena, Glue EventBridge, Secrets Manager). Diese Richtlinie sollte der Ausführungsrolle SageMaker Amazon-Domain/Benutzerprofil zugeordnet werden.

`AmazonSageMakerCanvasDataPrepFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerCanvasDataPrepFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Oktober 2023, 22:56 UTC

- Bearbeitete Zeit: 8. Dezember 2023, 02:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasDirectDeployAccess

Beschreibung: Ermöglicht Amazon SageMaker Canvas das Erstellen, Verwalten und Anzeigen von Endpunktdetails für Endgeräte, die mit Canvas erstellt wurden. Ermöglicht Amazon SageMaker Canvas das Abrufen von Endpunktaufrufmetriken von CloudWatch.

`AmazonSageMakerCanvasDirectDeployAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerCanvasDirectDeployAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Oktober 2023, 18:11 UTC
- Bearbeitete Zeit: 6. Oktober 2023, 18:11 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasForecastAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die üblicherweise für die Verwendung von SageMaker Canvas mit Amazon Forecast erforderlich sind.

`AmazonSageMakerCanvasForecastAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerCanvasForecastAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. August 2022, 20:04 UTC
- Bearbeitete Zeit: 24. August 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasFullAccess

Beschreibung: Bietet vollen Zugriff auf Ressourcen und Abläufe von Amazon SageMaker Canvas. Die Richtlinie bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager und Forecast). Diese Richtlinie sollte der Ausführungsrolle SageMaker Amazon-Domain/Benutzerprofil zugeordnet werden.

`AmazonSageMakerCanvasFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerCanvasFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. September 2022, 00:44 UTC
- Bearbeitete Zeit: 24. Januar 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:AddTags",
```

```
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*",
        "arn:aws:sagemaker:*:*:*model-compilation-*"
      ]
    },
    {
      "Sid" : "SageMakerHostingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:InvokeEndpointAsync"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*"
      ]
    },
    {
      "Sid" : "EC2VPCOperation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECROperations",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:GetBucketCors",
        "s3:GetBucketLocation"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : "glue:SearchTables",
      "Resource" : [
        "arn:aws:glue:*:*:table/*/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
```

```
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassOperationForForecast",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "application-autoscaling:scalable-dimension" :
"sagemaker:variant:DesiredInstanceCount"
        }
      }
    },
    {
      "Sid" : "AsyncEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "sagemaker:DescribeEndpointConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingSageMakerEndpointOperation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerClusterInstanceRolePolicy

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die üblicherweise für die Verwendung von Amazon SageMaker Cluster erforderlich sind.

`AmazonSageMakerClusterInstanceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerClusterInstanceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2023, 15:11 UTC
- Bearbeitete Zeit: 29. November 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCoreServiceRolePolicy

Beschreibung: Verwaltete Richtlinie für die serviceverknüpfte Rolle für Amazon SageMaker Core Services

`AmazonSageMakerCoreServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Dezember 2020, 21:40 Uhr UTC
- Bearbeitete Zeit: 21. Dezember 2020, 21:40 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerEdgeDeviceFleetPolicy

Beschreibung: Stellt die erforderlichen Berechtigungen bereit, damit SageMaker Edge mithilfe der Standard-Cloud-Verbindung eine Geräteflotte für den Kunden erstellen und verwalten kann.

`AmazonSageMakerEdgeDeviceFleetPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerEdgeDeviceFleetPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Dezember 2020, 16:17 Uhr UTC
- Zeit bearbeitet: 8. Dezember 2020, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerFeatureStoreAccess

Beschreibung: Stellt die erforderlichen Berechtigungen bereit, um den Offline-Shop für eine SageMaker FeatureStore Amazon-Feature-Gruppe zu aktivieren.

`AmazonSageMakerFeatureStoreAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerFeatureStoreAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 16:24 UTC
- Zeit bearbeitet: 5. Dezember 2022, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SageMaker über das AWS Management Console und SDK. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, ECR, CloudWatch Logs).

`AmazonSageMakerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 13:07 UTC
- Bearbeitete Zeit: 29. März 2024, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Version der Richtlinie

Richtlinienversion: v26 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowAddTagsForSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
```

```
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
```

```
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
```

```
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
```

```
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
```

```
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
```

```
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
```

```
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerGeospatialExecutionRole

Beschreibung: Diese Richtlinie ermöglicht den Zugriff auf Dienste, die häufig für die Verwendung von SageMaker Geodaten benötigt werden.

`AmazonSageMakerGeospatialExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerGeospatialExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 30. November 2022, 10:08 UTC
- Bearbeitete Zeit: 10. Mai 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerGeospatialFullAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die den vollen Zugriff auf Amazon SageMaker Geospatial über das SDK AWS Management Console und ermöglichen.

`AmazonSageMakerGeospatialFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerGeospatialFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 30. November 2022, 10:06 UTC
- Zeit bearbeitet: 30. November 2022, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerGroundTruthExecution

Beschreibung: Ermöglicht den Zugriff auf AWS Dienste, die für die Ausführung des SageMaker GroundTruth Labeling-Jobs erforderlich sind

`AmazonSageMakerGroundTruthExecution`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerGroundTruthExecution` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 09. Juli 2020, 19:30 Uhr UTC
- Bearbeitete Zeit: 29. April 2022, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerMechanicalTurkAccess

Beschreibung: Ermöglicht den Zugriff auf die Erstellung von Amazon Augmented FlowDefinition AI-Ressourcen für jedes Workteam.

`AmazonSageMakerMechanicalTurkAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerMechanicalTurkAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 16:19 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerModelGovernanceUseAccess

Beschreibung: Diese AWS verwaltete Richtlinie gewährt Berechtigungen, die für die Nutzung aller Amazon SageMaker Governance-Funktionen erforderlich sind. Die Richtlinie bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, KMS).

`AmazonSageMakerModelGovernanceUseAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerModelGovernanceUseAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2022, 08:58 UTC
- Bearbeitete Zeit: 4. Juni 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerModelRegistryFullAccess

Beschreibung: Dies ist eine neue verwaltete Richtlinie für Model Registry in Sagemaker. Bei dieser Richtlinie handelt es sich um eine eigenständige Richtlinie, die an die Benutzerrolle angehängt werden kann, um auf Funktionen im Zusammenhang mit Model Registry in Sagemaker zuzugreifen.

`AmazonSageMakerModelRegistryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerModelRegistryFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. April 2023, 05:20 UTC
- Bearbeitete Zeit: 6. Juni 2024, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerNotebooksServiceRolePolicy

Beschreibung: Verwaltete Richtlinie für Service Linked Role für Amazon SageMaker Notebooks

`AmazonSageMakerNotebooksServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. Oktober 2019, 20:27 UTC
- Bearbeitete Zeit: 22. Mai 2024, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEFSAccessPointCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
```

```
    },
    {
      "Sid" : "AllowEFSAccessPointDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSMountWithDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSDescribe",
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEFSTagging",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEC2Tagging",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowEC2Operations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowEC2AuthZ",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowIdcOperations",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSagemakerProfileCreation",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSagemakerSpaceOperationsForCanvasManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
```

```
        "sagemaker:DescribeSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*"
    },
    {
      "Sid" : "AllowSagemakerAddTagsForAppManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

Beschreibung: Richtlinie für Servicerollen, die vom AWS APIGateway innerhalb des AWS ServiceCatalog bereitgestellten SageMaker Produktportfolios von Amazon verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter Lambda und andere.

`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 01. August 2023, 15:06 UTC
- Bearbeitete Zeit: 1. August 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServi

Beschreibung: Servicerollenrichtlinie, die AWS CloudFormation vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Teilmenge verwandter Dienste, darunter Lambda, ApiGateway und andere.

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 01. August 2023, 15:06 UTC
- Bearbeitete Zeit: 1. August 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

Beschreibung: Richtlinie für Servicerollen, die von AWS Lambda in den AWS ServiceCatalog bereitgestellten Produkten aus dem SageMaker Amazon-Produktportfolio verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter Secrets Manager und andere.

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 01. August 2023, 15:05 UTC
- Bearbeitete Zeit: 1. August 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerPipelinesIntegrations

Beschreibung: Diese von Amazon Managed Policy gewährte Berechtigungen, die üblicherweise für die Verwendung mit Callback-Schritten und Lambda-Schritten in SageMaker Model Building-Pipelines benötigt werden. Sie wird dem hinzugefügt AmazonSageMaker — ExecutionRole das kann bei der Einrichtung von Studio erstellt werden. SageMaker Sie kann auch an jede andere Rolle angehängt werden, die für die Erstellung oder Ausführung von Pipelines verwendet wird.

`AmazonSageMakerPipelinesIntegrations`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerPipelinesIntegrations` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Juli 2021, 16:35 UTC
- Bearbeitete Zeit: 17. Februar 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerReadOnly

Beschreibung: Ermöglicht Lesezugriff auf Amazon SageMaker über das SDK AWS Management Console und.

`AmazonSageMakerReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 29. November 2017, 13:07 UTC
- Bearbeitete Zeit: 1. Dezember 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

Beschreibung: Service-Rollenrichtlinie, die vom AWS APIGateway innerhalb des AWS ServiceCatalog bereitgestellten SageMaker Produktportfolios von Amazon verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter CloudWatch Logs und andere.

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. März 2022, 04:25 UTC
- Bearbeitete Zeit: 25. März 2022, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

Beschreibung: Servicerollenrichtlinie, die AWS CloudFormation vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Teilmenge verwandter Dienste, darunter auch für andere SageMaker .

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. März 2022, 04:26 UTC
- Bearbeitete Zeit: 25. März 2022, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

Beschreibung: Servicerollenrichtlinie, die AWS CodeBuild vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Teilmenge verwandter Dienste CodePipeline, einschließlich CodeBuild und anderer.

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. März 2022, 04:27 UTC
- Bearbeitungszeit: 11. Juni 2024, 18:45 UTC

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

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

Beschreibung: Servicerollenrichtlinie, die AWS CodePipeline vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Teilmenge verwandter Dienste CodePipeline, einschließlich CodeBuild und anderer.

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. Februar 2022, 09:53 UTC
- Bearbeitete Zeit: 11. Juni 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
```

```
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
```

```
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Beschreibung: Servicerollenrichtlinie, die von den AWS CloudWatch Events innerhalb des AWS ServiceCatalog bereitgestellten SageMaker Produktportfolios von Amazon verwendet wird. Erteilt Berechtigungen für eine Teilmenge verwandter Dienste, darunter auch für andere CodePipeline .

`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. Februar 2022, 09:53 UTC
- Bearbeitete Zeit: 22. Februar 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Beschreibung: Richtlinie für Servicerollen, die von AWS Firehose im Rahmen des AWS ServiceCatalog bereitgestellten SageMaker Produktportfolios von Amazon verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter Firehose und andere.

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. Februar 2022, 09:54 UTC
- Bearbeitete Zeit: 22. Februar 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Beschreibung: Richtlinie für Servicerollen, die von AWS Glue im Rahmen des AWS ServiceCatalog bereitgestellten SageMaker Produktportfolios von Amazon verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter Glue, S3 und andere.

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. Februar 2022, 09:51 UTC
- Bearbeitete Zeit: 26. August 2022, 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Beschreibung: Richtlinie für Servicerollen, die von AWS Lambda in den AWS ServiceCatalog bereitgestellten Produkten aus dem SageMaker Amazon-Produktportfolio verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter ECR, S3 und andere.

`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. April 2022, 16:34 UTC
- Bearbeitungszeit: 11. Juni 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSecurityLakeAdministrator

Beschreibung: Bietet vollen Zugriff auf Amazon Security Lake und zugehörige Services, die für die Verwaltung von Security Lake erforderlich sind.

`AmazonSecurityLakeAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSecurityLakeAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2023, 22:04 UTC
- Bearbeitete Zeit: 23. Februar 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSecurityLakeMetastoreManager

Beschreibung: Richtlinie für Amazon SecurityLake Meta Store Manager Lambda, die den Zugriff auf Cloudwatch, S3, Glue und SQS ermöglicht.

`AmazonSecurityLakeMetastoreManager`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSecurityLakeMetastoreManager` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 23. Januar 2024, 15:26 UTC
- Bearbeitete Zeit: 1. April 2024, 20:04 UTC

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

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSecurityLakePermissionsBoundary

Beschreibung: Amazon Security Lake erstellt IAM-Rollen für benutzerdefinierte Quellen von Drittanbietern, um Daten in einen Data Lake zu schreiben, und für Drittanbieter-Abonnenten, um Daten aus einem Data Lake zu nutzen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenze ihrer Berechtigungen zu definieren.

`AmazonSecurityLakePermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSecurityLakePermissionsBoundary` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2022, 14:11 UTC
- Bearbeitete Zeit: 14. Mai 2024, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSESFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SES über die AWS Management Console.

`AmazonSESFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSESFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSESReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon SES über die AWS Management Console.

`AmazonSESReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSESReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 14. Mai 2024, 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSESServiceRolePolicy

Beschreibung: Ermöglicht SES, CloudWatch grundlegende Überwachungsmetriken von Amazon im Namen Ihrer SES-Ressourcen zu veröffentlichen

`AmazonSESServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Mai 2024, 16:02 UTC
- Bearbeitungszeit: 21. Mai 2024, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSNSFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SNS über die AWS Management Console.

`AmazonSNSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSNSFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSNSReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon SNS über die AWS Management Console.

`AmazonSNSReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSNSReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSNSRole

Beschreibung: Standardrichtlinie für die Amazon SNS SNS-Servicerolle.

`AmazonSNSRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSNSRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSQSFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SQS über die AWS Management Console.

`AmazonSQSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSQSFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSQSReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon SQS über die AWS Management Console.

`AmazonSQSReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSQSReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 24. Mai 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMAutomationApproverAccess

Beschreibung: Bietet Zugriff auf die Anzeige von Automatisierungsausführungen und das Senden von Genehmigungsentscheidungen an die Automatisierung, die auf ihre Genehmigung wartet

`AmazonSSMAutomationApproverAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSSMAutomationApproverAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. August 2017, 23:07 UTC
- Bearbeitete Zeit: 7. August 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution",
        "ssm:SendAutomationSignal"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMAutomationRole

Beschreibung: Stellt dem EC2 Automation-Dienst Berechtigungen zur Ausführung von Aktivitäten bereit, die in Automatisierungsdokumenten definiert sind

`AmazonSSMAutomationRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSSMAutomationRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Dezember 2016, 22:09 UTC
- Bearbeitete Zeit: 24. Juli 2017, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DeleteSnapshot",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
```

```
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:Automation*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMDirectoryServiceAccess

Beschreibung: Diese Richtlinie ermöglicht es dem SSM-Agenten, im Namen des Kunden auf den Directory Service zuzugreifen, um der verwalteten Instanz einen Domänenbeitritt zu ermöglichen.

`AmazonSSMDirectoryServiceAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSSMDirectoryServiceAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. März 2019, 17:44 Uhr UTC
- Bearbeitete Zeit: 15. März 2019, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SSM.

`AmazonSSMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSSMFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. Mai 2015, 17:39 Uhr UTC
- Bearbeitete Zeit: 20. November 2019, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMMaintenanceWindowRole

Beschreibung: Servicerolle, die für das EC2-Wartungsfenster verwendet werden soll

`AmazonSSMMaintenanceWindowRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSSMMaintenanceWindowRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2016, 15:57 Uhr UTC
- Bearbeitete Zeit: 27. Juli 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMManagedEC2InstanceDefaultPolicy

Beschreibung: Diese Richtlinie aktiviert die AWS Systems Manager Manager-Funktionalität auf EC2-Instances.

`AmazonSSMManagedEC2InstanceDefaultPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSSMManagedEC2InstanceDefaultPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. August 2022, 20:54 UTC
- Bearbeitete Zeit: 30. August 2022, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
```

```
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMManagedInstanceCore

Beschreibung: Die Richtlinie für die Amazon EC2 EC2-Rolle zur Aktivierung der Kernfunktionen des AWS Systems Manager Manager-Service.

`AmazonSSMManagedInstanceCore`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSSMManagedInstanceCore` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. März 2019, 17:22 Uhr UTC
- Bearbeitete Zeit: 23. Mai 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMPatchAssociation

Beschreibung: Ermöglichen Sie den Zugriff auf untergeordnete Instanzen für die Patchzuweisung.

`AmazonSSMPatchAssociation`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSSMPatchAssociation` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Mai 2020, 16:00 Uhr UTC
- Bearbeitete Zeit: 13. Mai 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon SSM.

`AmazonSSMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSSMReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. Mai 2015, 17:44 Uhr UTC
- Bearbeitete Zeit: 29. Mai 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMServiceRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von Amazon SSM verwaltet oder verwendet werden

`AmazonSSMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. November 2017, 19:20 Uhr UTC
- Bearbeitete Zeit: 14. September 2022, 19:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
```

```
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups: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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSumerianFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Sumerian.

`AmazonSumerianFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonSumerianFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. April 2018, 20:14 UTC
- Bearbeitete Zeit: 24. April 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "sumerian:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTextractFullAccess

Beschreibung: Zugriff auf alle Amazon Textract Textract-APIs

`AmazonTextractFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonTextractFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 19:07 UTC
- Bearbeitete Zeit: 28. November 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTextractServiceRole

Beschreibung: Ermöglicht Textract, AWS Dienste in Ihrem Namen anzurufen.

`AmazonTextractServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonTextractServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 28. November 2018, 19:12 Uhr UTC
- Zeit bearbeitet: 28. November 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung von Amazon Timestream mithilfe der AWS Management Console. Beachten Sie, dass diese Richtlinie auch Berechtigungen für bestimmte KMS-Operationen und Operationen zur Verwaltung Ihrer gespeicherten Abfragen gewährt. Wenn Sie vom Kunden verwaltetes CMK verwenden, finden Sie in der Dokumentation nach, welche zusätzlichen Berechtigungen erforderlich sind.

`AmazonTimestreamConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonTimestreamConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2020, 21:47 UTC
- Zeit bearbeitet: 1. Februar 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Timestream. Beachten Sie, dass diese Richtlinie auch Zugriff auf bestimmte KMS-Operationen gewährt. Wenn Sie vom Kunden verwaltetes CMK verwenden, finden Sie in der Dokumentation nach, welche zusätzlichen Berechtigungen erforderlich sind.

`AmazonTimestreamFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonTimestreamFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2020, 21:47 UTC
- Bearbeitete Zeit: 26. November 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamInfluxDBFullAccess

Beschreibung: Bietet vollen Administratorzugriff zum Erstellen, Aktualisieren, Löschen und Auflisten von Amazon Timestream InfluxDB-Instances sowie zum Erstellen und Auflisten von Parametergruppen. Weitere erforderliche Berechtigungen finden Sie in der Dokumentation.

`AmazonTimestreamInfluxDBFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonTimestreamInfluxDBFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. März 2024, 22:53 UTC
- Bearbeitete Zeit: 14. März 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
```

```
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance"
      ],
      "Resource" : [
        "arn:aws:timestream-influxdb:*:*:*"
      ]
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamInfluxDBServiceRolePolicy

Beschreibung: Bietet vollen Administratorzugriff zum Erstellen, Aktualisieren, Löschen und Auflisten von Amazon Timestream InfluxDB-Instances sowie zum Erstellen und Auflisten von Parametergruppen. Weitere erforderliche Berechtigungen finden Sie in der Dokumentation.

`AmazonTimestreamInfluxDBServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. März 2024, 18:53 UTC
- Bearbeitete Zeit: 14. März 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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}"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Timestream. Die Richtlinie gewährt auch die Erlaubnis, alle laufenden Abfragen abzubrechen. Wenn Sie vom Kunden verwaltetes CMK verwenden, finden Sie in der Dokumentation nach, welche zusätzlichen Berechtigungen erforderlich sind.

`AmazonTimestreamReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonTimestreamReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2020, 21:47 UTC
- Bearbeitete Zeit: 5. Juni 2024, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTranscribeFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Transcribe Transcribe-Operationen

`AmazonTranscribeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonTranscribeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. April 2018, 16:06 UTC
- Bearbeitete Zeit: 4. April 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTranscribeReadOnlyAccess

Beschreibung: Bietet Zugriff auf den schreibgeschützten Betrieb für Amazon Transcribe

`AmazonTranscribeReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonTranscribeReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. April 2018, 16:05 UTC
- Bearbeitete Zeit: 4. April 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCCrossAccountNetworkInterfaceOperations

Beschreibung: Ermöglicht den Zugriff auf die Erstellung von Netzwerkschnittstellen und deren Verknüpfung mit kontoübergreifenden Ressourcen

`AmazonVPCCrossAccountNetworkInterfaceOperations`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonVPCCrossAccountNetworkInterfaceOperations` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juli 2017, 20:47 UTC
- Bearbeitete Zeit: 25. September 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon VPC über die AWS Management Console.

`AmazonVPCFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonVPCFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 8. Februar 2024, 16:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
```

```
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpcPeeringConnection",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLink",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
```

```
        "ec2:EnableVpcClassicLink",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:RejectVpcPeeringConnection",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Beschreibung: Bietet Berechtigungen zum Beschreiben von AWS Ressourcen, zum Ausführen von Network Access Analyzer und zum Erstellen oder Löschen von Tags für Network Insights Access Scope und Network Insights Access Scope Analysis.

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Juni 2023, 22:56 UTC
- Bearbeitete Zeit: 15. Mai 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Beschreibung: Bietet Berechtigungen zum Beschreiben von AWS Ressourcen, zum Ausführen von Reachability Analyzer und zum Erstellen oder Löschen von Tags auf Network Insights Path und Network Insights Analysis.

`AmazonVPCReachabilityAnalyzerFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonVPCReachabilityAnalyzerFullAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Juni 2023, 20:12 UTC
- Bearbeitete Zeit: 15. Mai 2024, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Beschreibung: Diese Richtlinie ist der Rolle IAM RoleForReachabilityAnalyzerCrossAccountResourceAccess zugeordnet. Diese Rolle wird für die Mitgliedskonten in einer Organisation bereitgestellt, wenn das Verwaltungskonto den vertrauenswürdigen Zugriff für Reachability Analyzer ermöglicht. Es bietet Berechtigungen zum Anzeigen von Ressourcen aus Ihrer gesamten Organisation mithilfe der Reachability Analyzer-Konsole.

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Mai 2023, 20:38 UTC
- Bearbeitete Zeit: 1. Mai 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon VPC über die AWS Management Console.

`AmazonVPCReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonVPCReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 8. Februar 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
```

```
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkDocsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon WorkDocs über AWS Management Console

`AmazonWorkDocsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkDocsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. April 2020, 23:05 UTC
- Bearbeitete Zeit: 16. April 2020, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkDocsReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon WorkDocs über die AWS Management Console

`AmazonWorkDocsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkDocsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Januar 2020, 23:49 UTC
- Zeit bearbeitet: 8. Januar 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailEventsServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon WorkMail Events verwendet oder verwaltet werden

`AmazonWorkMailEventsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. April 2019, 16:52 UTC
- Bearbeitete Zeit: 16. April 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailFullAccess

Beschreibung: Bietet vollen Zugriff auf Directory Service WorkMail, SES, EC2 und Lesezugriff auf KMS-Metadaten.

`AmazonWorkMailFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkMailFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 21. Dezember 2020, 14:13 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailMessageFlowFullAccess

Beschreibung: Voller Zugriff auf die WorkMail Message Flow APIs

`AmazonWorkMailMessageFlowFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkMailMessageFlowFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Februar 2021, 11:08 UTC
- Bearbeitete Zeit: 11. Februar 2021, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailMessageFlowReadOnlyAccess

Beschreibung: Schreibgeschützter Zugriff auf WorkMail Nachrichten für die GetRawMessageContent API

`AmazonWorkMailMessageFlowReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkMailMessageFlowReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Januar 2021, 12:40 Uhr UTC

- Bearbeitete Zeit: 28. Januar 2021, 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf WorkMail und SES.

`AmazonWorkMailReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkMailReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 25. Juli 2019, 08:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesAdmin

Beschreibung: Bietet Zugriff auf WorkSpaces Amazon-Verwaltungsaktionen über AWS SDK und CLI.

`AmazonWorkSpacesAdmin`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkSpacesAdmin` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2015, 22:21 Uhr UTC
- Bearbeitete Zeit: 3. August 2023, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces:DeleteTags",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StopWorkspaces",
        "workspaces:TerminateWorkspaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesApplicationManagerAdminAccess

Beschreibung: Bietet Administratorzugriff für das Verpacken einer Anwendung in Amazon WorkSpaces Application Manager.

`AmazonWorkSpacesApplicationManagerAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkSpacesApplicationManagerAdminAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. April 2015, 14:03 UTC
- Bearbeitete Zeit: 9. April 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkspacesPCAAccess

Beschreibung: Diese verwaltete Richtlinie bietet vollen Administratorzugriff auf AWS Certificate Manager Private CA-Ressourcen in Ihrem AWS-Konto für die zertifikatsbasierte Authentifizierung.

`AmazonWorkspacesPCAAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkspacesPCAAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. November 2022, 00:25 UTC

- Zeit bearbeitet: 8. November 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesSelfServiceAccess

Beschreibung: Bietet Zugriff auf den WorkSpaces Amazon-Backend-Service zur Durchführung von Workspace Self Service-Aktionen

`AmazonWorkSpacesSelfServiceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkSpacesSelfServiceAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2019, 19:22 UTC
- Bearbeitete Zeit: 27. Juni 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesServiceAccess

Beschreibung: Ermöglicht Kundenkontozugriff auf den AWS WorkSpaces Service zum Starten eines Workspace.

`AmazonWorkSpacesServiceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkSpacesServiceAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2019, 19:19 UTC
- Zeit bearbeitet: 18. März 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesWebReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon WorkSpaces Web und seine Abhängigkeiten über das SDK und die AWS Management Console CLI.

`AmazonWorkSpacesWebReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonWorkSpacesWebReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2021, 14:20 Uhr UTC
- Zeit bearbeitet: 2. November 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesWebServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon WorkSpaces Web verwendet oder verwaltet werden

`AmazonWorkSpacesWebServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2021, 13:15 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonZocaloFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Zocalo.

`AmazonZocaloFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonZocaloFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonZocaloReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Zocalo

`AmazonZocaloReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmazonZocaloReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmplifyBackendDeployFullAccess

Beschreibung: Bietet Amplify-Vollzugriffsberechtigungen für die Bereitstellung von Amplify-Backend-Ressourcen (AWS AppSyncAmazon Cognito, Amazon S3 und andere verwandte Dienste) über das AWS Cloud Development Kit (CDK)AWS

`AmplifyBackendDeployFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AmplifyBackendDeployFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Oktober 2023, 21:32 UTC
- Bearbeitete Zeit: 31. Mai 2024, 15:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
```

```
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableFunctionResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*",
        "arn:aws:ssm:*:*:parameter/cdk-bootstrap/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AmplifyDiscoverRDSVpcConfig",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBProxies",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "ec2:DescribeSubnets",
        "rds:DescribeDBSubnetGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db-proxy:*",
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

APIGatewayServiceRolePolicy

Beschreibung: Ermöglicht API Gateway, zugehörige AWS Ressourcen im Namen des Kunden zu verwalten.

`APIGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Oktober 2017, 17:23 Uhr UTC
- Bearbeitete Zeit: 12. Juli 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AppIntegrationsServiceLinkedRolePolicy

Beschreibung: Ermöglicht AppIntegrations die Verwaltung von AppFlow Ressourcen und die Veröffentlichung von CloudWatch Metrikdaten in Ihrem Namen.

`AppIntegrationsServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. September 2022, 19:42 UTC
- Bearbeitete Zeit: 30. September 2022, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ApplicationAutoScalingForAmazonAppStreamAccess

Beschreibung: Richtlinie zur Aktivierung von Application Autoscaling für Amazon AppStream

`ApplicationAutoScalingForAmazonAppStreamAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ApplicationAutoScalingForAmazonAppStreamAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2017, 21:39 Uhr UTC
- Zeit bearbeitet: 6. Februar 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die Ressourcen, die von der Funktion Application Discovery Service Continuous Export verwendet oder verwaltet werden

`ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. August 2018, 20:22 UTC
- Bearbeitete Zeit: 13. August 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AppRunnerNetworkingServiceRolePolicy

Beschreibung: Ermöglicht AWS AppRunner Networking, verwandte AWS Ressourcen in Ihrem Namen zu verwalten.

`AppRunnerNetworkingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Januar 2022, 21:02 UTC
- Bearbeitete Zeit: 12. Januar 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AppRunnerServiceRolePolicy

Beschreibung: Ermöglicht AWS AppRunner die Verwaltung verwandter AWS Ressourcen in Ihrem Namen.

`AppRunnerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. Mai 2021, 19:15 UTC
- Bearbeitete Zeit: 14. Mai 2021, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Auto Scaling über die AWS Management Console.

`AutoScalingConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AutoScalingConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2017, 19:43 UTC
- Zeit bearbeitet: 6. Februar 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingConsoleReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Auto Scaling über die. AWS Management Console

`AutoScalingConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AutoScalingConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2017, 19:48 UTC
- Zeit bearbeitet: 12. Januar 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingFullAccess

Beschreibung: Bietet vollen Zugriff auf Auto Scaling.

`AutoScalingFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AutoScalingFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2017, 19:31 UTC
- Bearbeitete Zeit: 6. Februar 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingNotificationAccessRole

Beschreibung: Standardrichtlinie für die Servicerolle AutoScaling Notification Access.

`AutoScalingNotificationAccessRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AutoScalingNotificationAccessRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Auto Scaling.

`AutoScalingReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AutoScalingReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 12. Januar 2017, 19:39 UTC
- Zeit bearbeitet: 12. Januar 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Auto Scaling verwendet oder verwaltet werden

`AutoScalingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Januar 2018, 23:10 UTC
- Bearbeitete Zeit: 29. Februar 2024, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateFleet",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DetachClassicLinkVpc",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2InstanceProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "ELBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Register*",
        "elasticloadbalancing:Deregister*",
        "elasticloadbalancing:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSManagement",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "autoscaling.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "SystemsManagerParameterManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeManagement",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeregisterTargets",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListTargets",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWS_ConfigRole

Beschreibung: Standardrichtlinie für die AWS Config-Dienstrolle. Stellt die für AWS Config erforderlichen Berechtigungen bereit, um Änderungen an Ihren AWS Ressourcen nachzuverfolgen.

`AWS_ConfigRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWS_ConfigRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 15. September 2020, 20:30 Uhr UTC
- Bearbeitete Zeit: 22. Februar 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Version der Richtlinie

Richtlinienversion: v30 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
```

```
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "apigateway:GET",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
```

```
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
```

```
        "autoscaling:DescribeWarmPool",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
```

```
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
```

```
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
        "connect:DescribeQuickConnect",
        "connect:DescribeRule",
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
```

```
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQuickConnects",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
```

```
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
```

```
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
```

```
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
```

```
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
```

```
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
```

```
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
```

```
        "glue:ListMLTransforms",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
```

```
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
```

```
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
```

```
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
```

```
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:ListConnectors",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
```

```
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
```

```
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
```

```
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeFlow",
        "mediaconnect:ListFlows",
        "mediaconnect:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
```

```
            "network-firewall:ListFirewalls",
            "networkmanager:DescribeGlobalNetworks",
            "networkmanager:GetConnectPeer",
            "networkmanager:GetCustomerGatewayAssociations",
            "networkmanager:GetDevices",
            "networkmanager:GetLinkAssociations",
            "networkmanager:GetLinks",
            "networkmanager:GetSites",
            "networkmanager:GetTransitGatewayRegistrations",
            "networkmanager:ListConnectPeers",
            "networkmanager:ListTagsForResource",
            "nimble:GetLaunchProfile",
            "nimble:GetLaunchProfileDetails",
            "nimble:GetStreamingImage",
            "nimble:GetStudio",
            "nimble:GetStudioComponent",
            "nimble:ListLaunchProfiles",
            "nimble:ListStreamingImages",
            "nimble:ListStudioComponents",
            "nimble:ListStudios",
            "opsworks:DescribeInstances",
            "opsworks:DescribeLayers",
            "opsworks:DescribeTimeBasedAutoScaling",
            "opsworks:DescribeVolumes",
            "opsworks:ListTags",
            "organizations:DescribeAccount",
            "organizations:DescribeEffectivePolicy",
            "organizations:DescribeOrganization",
            "organizations:DescribeOrganizationalUnit",
            "organizations:DescribePolicy",
            "organizations:DescribeResourcePolicy",
            "organizations:ListAccounts",
            "organizations:ListAccountsForParent",
            "organizations:ListDelegatedAdministrators",
            "organizations:ListOrganizationalUnitsForParent",
            "organizations:ListParents",
            "organizations:ListPolicies",
            "organizations:ListPoliciesForTarget",
            "organizations:ListRoots",
            "organizations:ListTagsForResource",
            "organizations:ListTargetsForPolicy",
            "panorama:DescribeApplicationInstance",
            "panorama:DescribeApplicationInstanceDetails",
            "panorama:DescribePackage",
```

```
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
```

```
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
```

```
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
```

```
            "route53:GetDNSSEC",
            "route53:GetHealthCheck",
            "route53:GetHostedZone",
            "route53:ListCidrBlocks",
            "route53:ListCidrCollections",
            "route53:ListCidrLocations",
            "route53:ListHealthChecks",
            "route53:ListHostedZones",
            "route53:ListHostedZonesByName",
            "route53:ListQueryLoggingConfigs",
            "route53:ListResourceRecordSets",
            "route53:ListTagsForResource",
            "route53resolver:GetFirewallDomainList",
            "route53resolver:GetFirewallRuleGroup",
            "route53resolver:GetFirewallRuleGroupAssociation",
            "route53resolver:GetResolverDnssecConfig",
            "route53resolver:GetResolverEndpoint",
            "route53resolver:GetResolverQueryLogConfig",
            "route53resolver:GetResolverQueryLogConfigAssociation",
            "route53resolver:GetResolverRule",
            "route53resolver:GetResolverRuleAssociation",
            "route53resolver:ListFirewallDomainLists",
            "route53resolver:ListFirewallDomains",
            "route53resolver:ListFirewallRuleGroupAssociations",
            "route53resolver:ListFirewallRuleGroups",
            "route53resolver:ListFirewallRules",
            "route53resolver:ListResolverDnssecConfigs",
            "route53resolver:ListResolverEndpointIpAddresses",
            "route53resolver:ListResolverEndpoints",
            "route53resolver:ListResolverQueryLogConfigAssociations",
            "route53resolver:ListResolverQueryLogConfigs",
            "route53resolver:ListResolverRuleAssociations",
            "route53resolver:ListResolverRules",
            "route53resolver:ListTagsForResource",
            "rum:GetAppMonitor",
            "rum:GetAppMonitorData",
            "rum:ListAppMonitors",
            "rum:ListTagsForResource",
            "s3-outposts:GetAccessPoint",
            "s3-outposts:GetAccessPointPolicy",
            "s3-outposts:GetBucket",
            "s3-outposts:GetBucketPolicy",
            "s3-outposts:GetBucketTagging",
            "s3-outposts:GetLifecycleConfiguration",
```

```
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
```

```
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListTags",
        "sagemaker:ListWorkteams",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
```

```
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
        "sdb:ListDomains",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "serviceCatalog:DescribePortfolioShares",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTemplates",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeSubscription",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
```

```
        "sqs:ListQueueTags",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
```

```
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAccountActivityAccess

Beschreibung: Ermöglicht Benutzern den Zugriff auf die Seite mit den Kontoaktivitäten.

`AWSAccountActivityAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAccountActivityAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 7. März 2023, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAccountManagementFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS Kontoverwaltung.

`AWSAccountManagementFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAccountManagementFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2021, 23:20 Uhr UTC
- Bearbeitete Zeit: 30. September 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAccountManagementReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die Kontoverwaltung AWS

`AWSAccountManagementReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAccountManagementReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2021, 23:29 Uhr UTC
- Bearbeitete Zeit: 30. September 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAccountUsageReportAccess

Beschreibung: Ermöglicht Benutzern den Zugriff auf die Seite mit dem Kontonutzungsbericht.

`AWSAccountUsageReportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAccountUsageReportAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAgentlessDiscoveryService

Beschreibung: Ermöglicht den Zugriff für den Discovery Agentless Connector zur Registrierung beim AWS Application Discovery Service.

`AWSAgentlessDiscoveryService`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAgentlessDiscoveryService` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. August 2016, 01:35 UTC
- Bearbeitete Zeit: 24. Februar 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppFabricFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS AppFabric Dienst und schreibgeschützten Zugriff auf abhängige Dienste wie S3, Kinesis, KMS.

`AWSAppFabricFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppFabricFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2023, 19:51 UTC
- Bearbeitete Zeit: 27. Juni 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppFabricReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS AppFabric

`AWSAppFabricReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppFabricReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2023, 19:52 UTC
- Bearbeitete Zeit: 27. Juni 2023, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppFabricServiceRolePolicy

Beschreibung: Ermöglicht AppFabric den Zugriff auf AWS Ressourcen in Ihrem Namen

`AWSAppFabricServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. Juni 2023, 21:07 UTC
- Bearbeitete Zeit: 26. Juni 2023, 21:07 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingAppStreamFleetPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Zugriffsberechtigungen gewährt AppStream und CloudWatch.

`AWSApplicationAutoscalingAppStreamFleetPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Oktober 2017, 19:04 Uhr UTC

- Bearbeitete Zeit: 20. Oktober 2017, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingCassandraTablePolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Cassandra gewährt und CloudWatch.

`AWSApplicationAutoscalingCassandraTablePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. März 2020, 22:49 UTC
- Bearbeitete Zeit: 18. März 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingComprehendEndpointPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Comprehend und gewährt. CloudWatch

`AWSApplicationAutoscalingComprehendEndpointPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 14. November 2019, 18:39 Uhr UTC
- Bearbeitete Zeit: 14. November 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoScalingCustomResourcePolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf ApiGateway und CloudWatch für die benutzerdefinierte Ressourcenskalierung gewährt

`AWSApplicationAutoScalingCustomResourcePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. Juni 2018, 23:22 UTC
- Bearbeitete Zeit: 4. Juni 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingDynamoDBTablePolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf DynamoDB gewährt und. CloudWatch

`AWSApplicationAutoscalingDynamoDBTablePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 20. Oktober 2017, 21:34 UTC
- Zeit bearbeitet: 20. Oktober 2017, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf EC2 Spot Fleet gewährt und CloudWatch.

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Oktober 2017, 18:23 Uhr UTC
- Zeit bearbeitet: 25. Oktober 2017, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingECSServicePolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf den EC2 Container Service gewährt und CloudWatch.

`AWSApplicationAutoscalingECSServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Oktober 2017, 23:53 Uhr UTC
- Zeit bearbeitet: 25. Oktober 2017, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingElastiCacheRGPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Amazon ElastiCache und Amazon gewährt CloudWatch.

`AWSApplicationAutoscalingElastiCacheRGPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. August 2021, 23:41 UTC
- Bearbeitete Zeit: 17. August 2021, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameters",
        "cloudwatch:DescribeAlarms"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Zugriffsberechtigungen für Elastic Map Reduce gewährt und CloudWatch.

`AWSApplicationAutoscalingEMRInstanceGroupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 26. Oktober 2017, 00:57 UTC
- Zeit bearbeitet: 26. Oktober 2017, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingKafkaClusterPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Managed Streaming for Apache Kafka gewährt und CloudWatch.

`AWSApplicationAutoscalingKafkaClusterPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. August 2020, 18:36 Uhr UTC
- Zeit bearbeitet: 24. August 2020, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Lambda gewährt und CloudWatch.

`AWSApplicationAutoscalingLambdaConcurrencyPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Oktober 2019, 20:04 UTC
- Bearbeitete Zeit: 21. Oktober 2019, 20:04 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingNeptuneClusterPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Amazon Neptune und Amazon gewährt. CloudWatch

`AWSApplicationAutoscalingNeptuneClusterPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 02. September 2021, 21:14 UTC
- Bearbeitete Zeit: 02. September 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingRDSClusterPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf RDS gewährt und CloudWatch.

`AWSApplicationAutoscalingRDSClusterPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Oktober 2017, 17:46 Uhr UTC
- Bearbeitete Zeit: 7. August 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingSageMakerEndpointPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Zugriffsberechtigungen gewährt SageMaker und CloudWatch.

`AWSApplicationAutoscalingSageMakerEndpointPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. Februar 2018, 19:58 UTC
- Bearbeitete Zeit: 13. November 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationDiscoveryAgentAccess

Beschreibung: Ermöglicht dem Discovery Agent den Zugriff auf die Registrierung beim AWS Application Discovery Service.

`AWSApplicationDiscoveryAgentAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationDiscoveryAgentAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2016, 21:38 UTC
- Bearbeitete Zeit: 24. Februar 2020, 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationDiscoveryAgentlessCollectorAccess

Beschreibung: Ermöglicht Application Discovery Service Agentless Collectors die auto Aktualisierung, Registrierung und Kommunikation mit dem Application Discovery Service

`AWSApplicationDiscoveryAgentlessCollectorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationDiscoveryAgentlessCollectorAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. August 2022, 21:00 Uhr UTC
- Bearbeitete Zeit: 16. August 2022, 21:00 Uhr UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationDiscoveryServiceFullAccess

Beschreibung: Bietet vollen Zugriff auf das Anzeigen und Markieren von Konfigurationselementen, die vom AWS Application Discovery Service verwaltet werden

`AWSApplicationDiscoveryServiceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationDiscoveryServiceFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2016, 21:30 Uhr UTC
- Bearbeitete Zeit: 19. Juni 2019, 21:21 UTC

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

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationAgentInstallationPolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation des AWS Replication Agents, der zusammen mit dem AWS Application Migration Service (MGN) zur Migration externer Server

verwendet wird. AWS Ordnen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen zu, deren Anmeldeinformationen Sie bei der Installation des AWS Replication Agent angeben.

`AWSApplicationMigrationAgentInstallationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationAgentInstallationPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Juni 2022, 07:51 UTC
- Bearbeitete Zeit: 20. September 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationAgentPolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS Replication Agents, der zusammen mit dem AWS Application Migration Service (MGN) zur Migration externer Server verwendet wird. AWS Ordnen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen zu, deren Anmeldeinformationen Sie bei der Installation des AWS Replication Agent angeben.

`AWSApplicationMigrationAgentPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationAgentPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. April 2021, 07:00 UTC
- Bearbeitete Zeit: 20. September 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationAgentPolicy_v2

Beschreibung: Diese Richtlinie ermöglicht die Verwendung des AWS Replication Agents, der zusammen mit dem AWS Application Migration Service (MGN) verwendet wird, um externe Server zu AWS migrieren. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSApplicationMigrationAgentPolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationAgentPolicy_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Juni 2022, 14:14 UTC
- Bearbeitete Zeit: 6. Juni 2022, 14:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationConversionServerPolicy

Beschreibung: Diese Richtlinie ermöglicht dem Application Migration Service (MGN) Conversion Server, bei denen es sich um EC2-Instances handelt, die vom Application Migration Service gestartet werden, die Kommunikation mit dem MGN-Dienst. Eine IAM-Rolle mit dieser Richtlinie wird (als EC2-Instanzprofil) von MGN an die MGN Conversion Server angehängt, die bei Bedarf automatisch von MGN gestartet und beendet werden. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen. MGN Conversion Server werden vom Application Migration Service verwendet, wenn Benutzer Test- oder Cutover-Instances über die MGN-Konsole, CLI oder API starten möchten.

`AWSApplicationMigrationConversionServerPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationConversionServerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. April 2021, 06:48 UTC

- Bearbeitete Zeit: 7. April 2021, 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationEC2Access

Beschreibung: Diese Richtlinie stellt Amazon EC2 EC2-Operationen bereit, die erforderlich sind, um den Application Migration Service (MGN) zu verwenden, um die migrierten Server als EC2-Instances zu starten. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSApplicationMigrationEC2Access`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationEC2Access` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. April 2021, 07:05 UTC
- Bearbeitete Zeit: 6. Februar 2023, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationFullAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen für alle öffentlichen APIs von AWS Application Migration Service (MGN) sowie Berechtigungen zum Lesen von KMS-Schlüsselinformationen. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSApplicationMigrationFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. April 2021, 06:56 UTC
- Bearbeitete Zeit: 19. Mai 2024, 08:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
```

```
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Sid" : "VisualEditor14",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor15",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Sid" : "VisualEditor16",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Sid" : "VisualEditor17",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor18",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor19",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor20",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationMGHAccess

Beschreibung: Diese Richtlinie ermöglicht es dem AWS Application Migration Service (MGN), Metadaten über den Fortschritt von Servern, die mithilfe von MGN migriert werden, an AWS Migration Hub (MGH) zu senden. MGN erstellt automatisch eine IAM-Rolle mit dieser angehängten Richtlinie und übernimmt diese Rolle. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSApplicationMigrationMGHAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationMGHAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. April 2021, 07:10 UTC
- Bearbeitete Zeit: 7. April 2021, 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen für alle schreibgeschützten öffentlichen APIs von Application Migration Service (MGN) sowie für einige schreibgeschützte APIs anderer AWS Dienste, die erforderlich sind, um die MGN-Konsole vollständig schreibgeschützt nutzen zu können. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSApplicationMigrationReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. April 2021, 07:15 UTC
- Bearbeitete Zeit: 20. März 2023, 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationReplicationServerPolicy

Beschreibung: Diese Richtlinie ermöglicht es den Application Migration Service (MGN) Replication Servern, bei denen es sich um vom Application Migration Service gestartete EC2-Instances handelt, mit dem MGN-Dienst zu kommunizieren und EBS-Snapshots in Ihrem zu erstellen. AWS-Konto Eine IAM-Rolle mit dieser Richtlinie wird (als EC2-Instanzprofil) vom Application Migration Service den MGN Replication Servern zugewiesen, die bei Bedarf automatisch von MGN gestartet und beendet werden. MGN Replication Server werden verwendet, um die Datenreplikation von Ihren externen Servern zu AWS erleichtern. Dies ist Teil des mit MGN verwalteten Migrationsprozesses. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSApplicationMigrationReplicationServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationReplicationServerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. April 2021, 07:21 UTC
- Bearbeitete Zeit: 7. April 2021, 07:21 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationServiceEc2InstancePolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS Replication Agents, der vom AWS Application Migration Service (AWS MGN) zur Migration von Quellservern verwendet wird, die auf EC2 ausgeführt werden (regionsübergreifend oder azübergreifend). Eine IAM-Rolle mit dieser Richtlinie sollte den EC2-Instances (als EC2-Instance-Profil) zugewiesen werden.

`AWSApplicationMigrationServiceEc2InstancePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationServiceEc2InstancePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. August 2023, 13:19 UTC
- Bearbeitete Zeit: 03. Januar 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationServiceRolePolicy

Beschreibung: Ermöglicht dem AWS Anwendungsmigrationsdienst, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

`AWSApplicationMigrationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. April 2021, 06:43 UTC
- Bearbeitete Zeit: 20. Juni 2023, 09:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationSSMAccess

Beschreibung: Diese Richtlinie bietet Zugriff auf Amazon SSM-Operationen, die für die Verwendung des Application Migration Service (MGN) zur Ausführung benutzerdefinierter SSM-Dokumente nach der Migration erforderlich sind. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSApplicationMigrationSSMAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationSSMAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 09:29 UTC
- Bearbeitete Zeit: 20. März 2023, 10:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationVCenterClientPolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS vCenter Client, der zusammen mit dem AWS Application Migration Service (MGN) zur Migration externer Server verwendet wird. AWS Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu, deren Anmeldeinformationen Sie bei der AWS Installation des vCenter Client angeben.

`AWSApplicationMigrationVCenterClientPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSApplicationMigrationVCenterClientPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. November 2021, 12:53 UTC
- Bearbeitete Zeit: 8. November 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshEnvoyAccess

Beschreibung: App Mesh Envoy-Richtlinie für den Zugriff auf die Konfiguration des virtuellen Knotens.

`AWSAppMeshEnvoyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppMeshEnvoyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Juli 2019, 21:29 Uhr UTC
- Bearbeitete Zeit: 3. Juli 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS App Mesh Mesh-APIs und die Management Console.

`AWSAppMeshFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppMeshFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. April 2019, 17:50 Uhr UTC
- Bearbeitete Zeit: 7. Januar 2021, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshPreviewEnvoyAccess

Beschreibung: App Mesh Preview Envoy-Richtlinie für den Zugriff auf die Konfiguration des virtuellen Knotens.

`AWSAppMeshPreviewEnvoyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppMeshPreviewEnvoyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. August 2019, 23:32 UTC
- Zeit bearbeitet: 5. August 2019, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshPreviewServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von AWS App Mesh verwendet oder verwaltet werden

`AWSAppMeshPreviewServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Juni 2019, 19:07 UTC
- Bearbeitete Zeit: 21. August 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS App Mesh Mesh-APIs und die Management Console.

`AWSAppMeshReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppMeshReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. April 2019, 17:51 UTC
- Bearbeitete Zeit: 7. Januar 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von verwendet oder verwaltet werden AWS AppMesh

`AWSAppMeshServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Juni 2019, 18:30 Uhr UTC
- Bearbeitete Zeit: 10. Oktober 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppRunnerFullAccess

Beschreibung: Erteilt Berechtigungen für alle App Runner-Aktionen.

`AWSAppRunnerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppRunnerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Januar 2022, 04:02 UTC
- Bearbeitete Zeit: 11. Januar 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppRunnerReadOnlyAccess

Beschreibung: Erteilt Berechtigungen zum Auflisten und Anzeigen von Details zu App Runner-Ressourcen.

`AWSAppRunnerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppRunnerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Februar 2022, 21:24 UTC
- Bearbeitete Zeit: 24. Februar 2022, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppRunnerServicePolicyForECRAccess

Beschreibung: AWS App Runner-Servicerichtlinie, die Leseberechtigungen für Amazon ECR-Ressourcen im Kundenkonto gewährt. Verwenden Sie es in einer Rolle, die bei der Erstellung oder Aktualisierung eines App Runner-Service an App Runner übergeben wird.

`AWSAppRunnerServicePolicyForECRAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppRunnerServicePolicyForECRAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Mai 2021, 19:17 UTC
- Bearbeitete Zeit: 14. Mai 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncAdministrator

Beschreibung: Bietet Administratorzugriff auf den AppSync Dienst, reicht jedoch nicht aus, um über die Konsole darauf zuzugreifen.

`AWSAppSyncAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppSyncAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 20. März 2018, 21:20 Uhr UTC
- Zeit bearbeitet: 4. November 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncInvokeFullAccess

Beschreibung: Bietet vollen Aufrufzugriff auf den AppSync Dienst — sowohl über die Konsole als auch unabhängig

`AWSAppSyncInvokeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppSyncInvokeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. März 2018, 21:21 Uhr UTC
- Bearbeitete Zeit: 20. März 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncPushToCloudWatchLogs

Beschreibung: Ermöglicht AppSync das Senden von Protokollen an das CloudWatch Benutzerkonto.

`AWSAppSyncPushToCloudWatchLogs`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppSyncPushToCloudWatchLogs` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 9. April 2018, 19:38 UTC
- Bearbeitete Zeit: 9. April 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncSchemaAuthor

Beschreibung: Ermöglicht den Zugriff zum Erstellen, Aktualisieren und Abfragen des Schemas.

`AWSAppSyncSchemaAuthor`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAppSyncSchemaAuthor` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. März 2018, 21:21 Uhr UTC
- Bearbeitete Zeit: 1. Februar 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Dienste und Ressourcen, die verwendet oder verwaltet werden von AppSync

`AWSAppSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Januar 2020, 19:56 UTC
- Bearbeitete Zeit: 21. Januar 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSArtifactAccountSync

Beschreibung: Ermöglicht AWS Artifact den schreibgeschützten Zugriff auf Operationen in Organizations. AWS

`AWSArtifactAccountSync`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSArtifactAccountSync` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. April 2018, 23:04 UTC
- Bearbeitete Zeit: 10. April 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSArtifactReportsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS Artifact-Serviceberichte.

`AWSArtifactReportsReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSArtifactReportsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. Januar 2024, 22:42 UTC
- Bearbeitete Zeit: 2. Januar 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSArtifactServiceRolePolicy

Beschreibung: Ermöglicht AWS Artifact, Informationen über eine Organisation über den AWS Organisationsdienst zu sammeln.

`AWSArtifactServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. August 2023, 20:27 UTC
- Bearbeitete Zeit: 21. August 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAuditManagerAdministratorAccess

Beschreibung: Bietet Administratorzugriff, um AWS Audit Manager zu aktivieren oder zu deaktivieren, Einstellungen zu aktualisieren und Bewertungen, Kontrollen und Frameworks zu verwalten

`AWSAuditManagerAdministratorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSAuditManagerAdministratorAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2020, 20:02 Uhr UTC
- Bearbeitete Zeit: 15. Mai 2024, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAuditManagerServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die Ressourcen, die von AWS Audit Manager verwendet oder verwaltet werden

`AWSAuditManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Dezember 2020, 15:12 Uhr UTC
- Bearbeitete Zeit: 10. Juni 2024, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeTableReplicaAutoScaling",
```

```
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:GetLaunchTemplateData",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
```

```
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccessKeyLastUsed",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListAccessKeys",
        "iam:ListAttachedRolePolicies",
        "iam:ListMfaDeviceTags",
        "iam:ListMfaDevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
```

```
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "es:DescribeDomains",
        "es:DescribeDomain",
        "es:DescribeDomainConfig",
        "es:ListDomainNames",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeLoggingStatus",
        "route53:GetQueryLoggingConfig",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeTrainingJob",
```

```
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListModels",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListUserProfiles",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "securityhub:DescribeStandards",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetRule",
        "waf-regional:GetWebAcl",
        "waf:GetRule",
        "waf:GetRuleGroup",
        "waf:ListActivatedRulesInRuleGroup",
        "waf:ListWebAcls",
        "wafv2:ListWebAcls",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf-regional:ListRules",
        "waf:ListRuleGroups",
        "waf:ListRules"
      ],
      "Resource" : "*",
      "Sid" : "APIsAccess"
```

```
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLogging",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
```

```
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:source" : "false"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAutoScalingPlansEC2AutoScalingPolicy

Beschreibung: Richtlinie, die AWS Auto Scaling berechtigt, die Kapazität regelmäßig zu prognostizieren und geplante Skalierungsaktionen für Auto Scaling Scaling-Gruppen in einem Skalierungsplan zu generieren

`AWSAutoScalingPlansEC2AutoScalingPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. August 2018, 22:46 Uhr UTC
- Bearbeitete Zeit: 23. August 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupAuditAccess

Beschreibung: Diese Richtlinie gewährt Benutzern die Erlaubnis, Kontrollen und Frameworks zu erstellen, die ihre Erwartungen an AWS Backup-Ressourcen und -Aktivitäten definieren, und AWS Backup-Ressourcen und -Aktivitäten anhand ihrer definierten Kontrollen und Frameworks zu überprüfen. Diese Richtlinie gewährt AWS Config und ähnlichen Diensten die Erlaubnis, die Erwartungen der Benutzer bei der Durchführung der Audits zu beschreiben. Diese Richtlinie gewährt auch Berechtigungen zur Übermittlung von Auditberichten an S3 und ähnliche Dienste und ermöglicht es Benutzern, ihre Auditberichte zu finden und zu öffnen.

`AWSBackupAuditAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupAuditAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. August 2021, 01:02 UTC

- Bearbeitete Zeit: 10. April 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupDataTransferAccess

Beschreibung: Diese Richtlinie ermöglicht es dem AWS Backint-Agenten, die Backup-Datenübertragung mit der AWS Backup-Speicherebene abzuschließen. Hängen Sie diese Richtlinie an Rollen an, die von EC2-Instances übernommen wurden, auf denen SAP HANA mit dem Backint-Agenten ausgeführt wird.

`AWSBackupDataTransferAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupDataTransferAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2022, 22:48 UTC
- Bearbeitete Zeit: 10. November 2022, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupFullAccess

Beschreibung: Diese Richtlinie richtet sich an Backup-Administratoren und gewährt vollen Zugriff auf AWS Backup-Operationen, darunter das Erstellen oder Bearbeiten von Backup-Plänen, das Zuweisen von AWS Ressourcen zu Backup-Plänen, das Löschen von Backups und das Wiederherstellen von Backups.

`AWSBackupFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. November 2019, 22:21 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Version der Richtlinie

Richtlinienversion: v17 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDbPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDbDeleteBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EfsFileSystemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
```

```
    },
    {
      "Sid" : "Ec2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2DeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ResourceGroupTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListVolumes",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "IamRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
```

```
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AwsOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemManagerCommandPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemManagerSendCommandPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeBackups",
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "DirectoryServicePermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "IamCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BackupGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:AssociateGatewayToServer",
        "backup-gateway:CreateGateway",
        "backup-gateway:DeleteGateway",
        "backup-gateway:DeleteHypervisor",
        "backup-gateway:DisassociateGatewayFromServer",
        "backup-gateway:ImportHypervisorConfiguration",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup-gateway:PutMaintenanceStartTime",
        "backup-gateway:TagResource",
        "backup-gateway:TestHypervisorConfiguration",
        "backup-gateway:UntagResource",
        "backup-gateway:UpdateGatewayInformation",
        "backup-gateway:UpdateHypervisor"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "BackupGatewayHypervisorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:PutHypervisorPropertyMappings",
        "backup-gateway:StartVirtualMachinesMetadataSync"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayVirtualMachinePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:PutBandwidthRateLimitSchedule"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListTables",
        "timestream:ListDatabases"
      ],
      "Resource" : [
```

```
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SystemsManagerForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceAccessManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Beschreibung: AWS BackupGateway Erlaubt die Erlaubnis, die Metadaten virtueller Maschinen in Ihrem Namen zu synchronisieren

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 15. Dezember 2022, 19:43 UTC
- Bearbeitete Zeit: 15. Dezember 2022, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupOperatorAccess

Beschreibung: Diese Richtlinie gewährt Benutzern die Berechtigung, AWS Ressourcen Backup-Plänen zuzuweisen, On-Demand-Backups zu erstellen und Backups wiederherzustellen. Diese Richtlinie erlaubt es dem Benutzer nicht, Backup-Pläne zu erstellen oder zu bearbeiten oder geplante Backups zu löschen, nachdem sie erstellt wurden.

`AWSBackupOperatorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupOperatorAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. November 2019, 22:23 Uhr UTC
- Bearbeitete Zeit: 6. September 2023, 20:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:CreateBackupSelection",
        "backup:DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
```

```
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListVolumes",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "fsx:DescribeStorageVirtualMachines",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
```

```
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupOrganizationAdminAccess

Beschreibung: Diese Richtlinie richtet sich an Backup-Administratoren, die kontoübergreifendes Backup-Management verwenden, um Backups für das Unternehmen zu verwalten.

`AWSBackupOrganizationAdminAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupOrganizationAdminAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 16:23 UTC
- Zeit bearbeitet: 18. November 2022, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupRestoreAccessForSAPHANA

Beschreibung: Bietet die AWS Backup-Berechtigung zum Wiederherstellen einer Sicherung von SAP HANA auf Amazon EC2

`AWSBackupRestoreAccessForSAPHANA`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupRestoreAccessForSAPHANA` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2022, 22:43 UTC
- Zeit bearbeitet: 10. November 2022, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceLinkedRolePolicyForBackup

Beschreibung: Bietet die AWS Backup-Berechtigung, um in Ihrem Namen Backups für alle AWS Dienste zu erstellen

`AWSBackupServiceLinkedRolePolicyForBackup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Juni 2020, 23:08 UTC
- Bearbeitete Zeit: 17. Mai 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Version der Richtlinie

Richtlinienversion: v16 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
```

```
    },
    {
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSBackupManagedResource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "RDSInstanceAndSnashotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBSnapshot",
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBInstanceAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot"
```

```
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CopyBackup",
        "fsx:TagResource",
        "fsx:DescribeBackups",
        "fsx:DeleteBackup"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
```

```
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeTable",
        "timestream:GetAwsBackupStatus",
        "timestream:GetAwsRestoreStatus"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
```

```
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceLinkedRolePolicyForBackupTest

Beschreibung: Bietet die AWS Backup-Berechtigung, um in Ihrem Namen Backups für alle AWS Dienste zu erstellen

`AWSBackupServiceLinkedRolePolicyForBackupTest`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Mai 2020, 17:37 UTC
- Bearbeitete Zeit: 12. Mai 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForBackup

Beschreibung: Bietet die AWS Backup-Berechtigung, um in Ihrem Namen Backups für alle AWS Dienste zu erstellen

`AWSBackupServiceRolePolicyForBackup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupServiceRolePolicyForBackup` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 10. Januar 2019, 21:01 UTC
- Bearbeitete Zeit: 17. Mai 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Version der Richtlinie

Richtlinienversion: v19 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RDSClusterBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
    },
    {
      "Sid" : "RDSBackupPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "RDSClusterModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EBSTagAndDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:image/*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotTierPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "BackupVaultPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource" : "arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Sid" : "BackupVaultCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CopyFromBackupVault"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
```

```
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EBSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
```

```
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSDataKeyEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSendPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
```

```
      ]
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxCreateBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:CreateBackup",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxListTagsPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:ListTagsForResource",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
```

```
    },
    {
      "Sid" : "FsxResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamodbBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:ListTagsOfResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "BackupGatewayBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
    },
    {
      "Sid" : "RedshiftCreatePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift:CreateClusterSnapshot",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForRestores

Beschreibung: Bietet die AWS Backup-Berechtigung, in Ihrem Namen wiederherzustellende AWS Dienste durchzuführen. Diese Richtlinie umfasst Berechtigungen zum Erstellen und Löschen von AWS Ressourcen wie EBS-Volumes, RDS-Instances und EFS-Dateisystemen, die Teil des Wiederherstellungsprozesses sind.

`AWSBackupServiceRolePolicyForRestores`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupServiceRolePolicyForRestores` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. Januar 2019, 00:23 UTC

- Bearbeitete Zeit: 15. Dezember 2023, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Version der Richtlinie

Richtlinienversion: v20 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
```

```
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:AddTagsToResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "RDSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:DeleteDBCluster",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:TagResource"
```

```
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "EBSSnapshotBlockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:CompleteSnapshot",
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "RDSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "EC2DeleteAndRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:RestoreSnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsScopedPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TerminateInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateVolume"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "fsx:CreateFileSystemFromBackup"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Sid" : "FsxTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "FsxDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
```

```
    {
      "Sid" : "FsxVolumeTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "FsxBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DSPermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromAwsBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "GatewayRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Restore"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "CloudformationChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:RestoreFromClusterSnapshot",
        "redshift:RestoreTableFromClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
```

```
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeTableRestoreStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsRestoreJob",
        "timestream:GetAwsRestoreStatus",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:ListDatabases",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : [
        "*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForS3Backup

Beschreibung: Richtlinie mit den für AWS Backup erforderlichen Berechtigungen zum Sichern von Daten in einem beliebigen S3-Bucket. Dazu gehören der Lesezugriff auf alle S3-Objekte und der Entschlüsselungszugriff für alle KMS-Schlüssel.

`AWSBackupServiceRolePolicyForS3Backup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupServiceRolePolicyForS3Backup` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Februar 2022, 17:40 UTC
- Bearbeitete Zeit: 17. Mai 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForS3Restore

Beschreibung: Richtlinie mit Berechtigungen, die AWS Backup benötigt, um ein S3-Backup in einem Bucket wiederherzustellen. Dazu gehören Lese-/Schreibberechtigungen für alle S3-Buckets sowie Berechtigungen DescribeKey für GenerateDataKey und für alle KMS-Schlüssel.

`AWSBackupServiceRolePolicyForS3Restore`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBackupServiceRolePolicyForS3Restore` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Februar 2022, 17:39 UTC
- Bearbeitete Zeit: 7. Februar 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBatchFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Batch-Ressourcen.

`AWSBatchFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBatchFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2016, 19:35 UTC
- Bearbeitete Zeit: 24. Oktober 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBatchServiceEventTargetRole

Beschreibung: Richtlinie zur Aktivierung von CloudWatch Event Target für die Einreichung von AWS Batch-Jobs

`AWSBatchServiceEventTargetRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBatchServiceEventTargetRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 28. Februar 2018, 22:31 UTC
- Bearbeitete Zeit: 28. Februar 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBatchServiceRole

Beschreibung: Richtlinie für die AWS Batch-Servicerolle, die den Zugriff auf verwandte Dienste wie EC2, Autoscaling, EC2 Container Service und Cloudwatch Logs ermöglicht.

`AWSBatchServiceRole`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBatchServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Dezember 2016, 19:36 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBCMDataExportsServiceRolePolicy

Beschreibung: Eine serviceverknüpfte Rolle, die Abrechnungs- und Kostenmanagement-Datenexporten Zugriff auf AWS Servicedaten ermöglicht, um die Daten im Namen eines Kunden an einen Zielort wie Amazon S3 zu exportieren.

`AWSBCMDataExportsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Juni 2024, 17:40 UTC
- Bearbeitete Zeit: 10. Juni 2024, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBillingConductorFullAccess

Beschreibung: Verwenden Sie die AWSBillingConductorFullAccess verwaltete Richtlinie, um vollständigen Zugriff auf die AWS Billing Conductor (ABC-) Konsole und die APIs zu gewähren. Diese Richtlinie ermöglicht es Benutzern, ABC-Ressourcen aufzulisten, zu erstellen und zu löschen.

`AWSBillingConductorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBillingConductorFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. April 2022, 18:02 UTC
- Bearbeitete Zeit: 13. April 2022, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBillingConductorReadOnlyAccess

Beschreibung: Verwenden Sie die AWSBillingConductorReadOnlyAccess verwaltete Richtlinie, um nur Lesezugriff auf die AWS Billing Conductor (ABC-) Konsole und APIs zu gewähren. Diese Richtlinie gewährt die Berechtigung zum Anzeigen und Auflisten aller ABC-Ressourcen. Sie beinhaltet nicht die Möglichkeit, Ressourcen zu erstellen oder zu löschen.

`AWSBillingConductorReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBillingConductorReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. April 2022, 18:02 UTC
- Bearbeitete Zeit: 13. April 2022, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBillingReadOnlyAccess

Beschreibung: Ermöglicht Benutzern, Rechnungen in der Abrechnungskonsole einzusehen.

`AWSBillingReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBillingReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. August 2020, 20:08 UTC
- Bearbeitete Zeit: 23. Mai 2024, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
```

```
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "budgets:ViewBudget",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:ListTagsForResource",
        "payments:ListPaymentInstruments",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
```

```
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Beschreibung: Diese Richtlinie gewährt Berechtigungen zur Steuerung von AWS Ressourcen. Zum Beispiel, um EC2- oder RDS-Instances zu starten und zu stoppen, indem AWS Systems Manager (SSM) -Skripts ausgeführt werden.

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Mai 2022, 19:03 UTC

- Bearbeitete Zeit: 25. Mai 2022, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBudgetsActionsWithAWSResourceControlAccess

Beschreibung: Bietet vollen Zugriff auf AWS Budgetaktionen, einschließlich der Verwendung von Budgetaktionen zur Steuerung des Status laufender AWS Ressourcen über AWS Management Console

`AWSBudgetsActionsWithAWSResourceControlAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBudgetsActionsWithAWSResourceControlAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Oktober 2020, 17:19 Uhr UTC
- Zeit bearbeitet: 15. Oktober 2020, 17:19 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBudgetsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS Budget-Konsole über die AWS Management Console.

`AWSBudgetsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBudgetsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Oktober 2020, 17:18 Uhr UTC
- Zeit bearbeitet: 15. Oktober 2020, 17:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBugBustFullAccess

Beschreibung: Diese IAM-Richtlinie gewährt Benutzern vollen Zugriff auf die Konsole AWS BugBust

`AWSBugBustFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBugBustFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2021, 07:03 UTC
- Bearbeitete Zeit: 22. Juli 2021, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBugBustPlayerAccess

Beschreibung: Diese IAM-Richtlinie gewährt Benutzern Zugriff auf die Teilnahme AWS BugBust an Veranstaltungen

`AWSBugBustPlayerAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSBugBustPlayerAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2021, 07:15 Uhr UTC
- Bearbeitete Zeit: 24. Juni 2021, 07:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBugBustServiceRolePolicy

Beschreibung: Erteilt die Erlaubnis AWS BugBust , in Ihrem Namen auf Ressourcen zuzugreifen

`AWSBugBustServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Juni 2021, 06:59 UTC
- Bearbeitete Zeit: 24. Juni 2021, 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Certificate Manager (ACM)

`AWSCertificateManagerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCertificateManagerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Januar 2016, 17:02 UTC
- Bearbeitete Zeit: 17. August 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAAuditor

Beschreibung: Bietet Auditor-Zugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAAuditor`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCertificateManagerPrivateCAAuditor` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Oktober 2018, 16:51 UTC
- Bearbeitete Zeit: 17. August 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCertificateManagerPrivateCAFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Oktober 2018, 16:54 UTC
- Bearbeitete Zeit: 23. Oktober 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAPrivilegedUser

Beschreibung: Bietet privilegierten Zertifikatsbenutzern Zugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAPrivilegedUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCertificateManagerPrivateCAPrivilegedUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. Juni 2019, 17:43 UTC
- Bearbeitete Zeit: 20. Juni 2019, 17:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCertificateManagerPrivateCAReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Oktober 2018, 16:57 UTC
- Bearbeitete Zeit: 17. August 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAUser

Beschreibung: Bietet Zertifikatsbenutzerzugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCertificateManagerPrivateCAUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Oktober 2018, 16:53 UTC
- Bearbeitete Zeit: 20. Juni 2019, 17:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Certificate Manager (ACM).

`AWSCertificateManagerReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCertificateManagerReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Januar 2016, 17:07 UTC
- Bearbeitete Zeit: 15. März 2021, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSChatbotServiceLinkedRolePolicy

Beschreibung: Die vom AWS Chatbot verwendete serviceverknüpfte Rolle.

`AWSChatbotServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2019, 16:39 Uhr UTC
- Bearbeitete Zeit: 18. November 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsFullAccess

Beschreibung: Ermöglicht den vollen Zugriff auf AWS Clean Rooms-Ressourcen und den Zugriff auf verwandte Ressourcen AWS-Services.

`AWSCleanRoomsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCleanRoomsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2023, 16:10 UTC
- Bearbeitete Zeit: 21. März 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsFullAccessNoQuerying

Beschreibung: Ermöglicht vollen Zugriff auf AWS Clean Rooms-Ressourcen mit Ausnahme von Abfragen in einer Kollaboration und Zugriff auf verwandte AWS-Services Ressourcen.

`AWSCleanRoomsFullAccessNoQuerying`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCleanRoomsFullAccessNoQuerying` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2023, 16:12 UTC
- Bearbeitete Zeit: 14. Mai 2024, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
```

```
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
        "cleanrooms:StartProtectedQuery",
        "cleanrooms:UpdateProtectedQuery"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
```

```
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsMLFullAccess

Beschreibung: Ermöglicht den vollen Zugriff auf AWS Clean Rooms ML-Ressourcen und den Zugriff auf verwandte AWS-Services.

`AWSCleanRoomsMLFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCleanRoomsMLFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2023, 21:02 UTC
- Bearbeitete Zeit: 29. November 2023, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
```

```
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CollaborationMembershipCheck",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:ListMembers"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cleanrooms-ml.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AssociateModels",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:CreateConfiguredAudienceModelAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAssociations",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:TagResource"
      ],
```

```
      "Resource" : "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cleanrooms-ml*",
        "arn:aws:iam::*:role/role/cleanrooms-ml*"
      ]
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanroomsml*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickOutputBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickS3Location",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*cleanrooms-ml*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsMLReadOnlyAccess

Beschreibung: Ermöglicht den schreibgeschützten Zugriff auf AWS Clean Rooms-ML-Ressourcen und den schreibgeschützten Zugriff auf zugehörige Clean Rooms-Ressourcen AWS

`AWSCleanRoomsMLReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCleanRoomsMLReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2023, 20:55 UTC
- Bearbeitete Zeit: 29. November 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsReadOnlyAccess

Beschreibung: Ermöglicht den schreibgeschützten Zugriff auf AWS Clean Rooms-Ressourcen und den schreibgeschützten Zugriff auf zugehörige AWS Glue- und Amazon Logs-Ressourcen. CloudWatch

`AWSCleanRoomsReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCleanRoomsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2023, 16:10 UTC
- Bearbeitete Zeit: 12. Januar 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9Administrator

Beschreibung: Bietet Administratorzugriff auf AWS Cloud9.

`AWSCloud9Administrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloud9Administrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:17 UTC
- Bearbeitete Zeit: 11. Oktober 2023, 12:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9EnvironmentMember

Beschreibung: Bietet die Möglichkeit, in gemeinsam genutzte AWS Cloud9-Entwicklungsumgebungen eingeladen zu werden.

`AWSCloud9EnvironmentMember`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloud9EnvironmentMember` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:18 Uhr UTC
- Bearbeitete Zeit: 11. Oktober 2023, 12:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "iam:GetUser",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
```

```
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9ServiceRolePolicy

Beschreibung: Service Linked Role Policy für AWS Cloud9

`AWSCloud9ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2017, 13:44 Uhr UTC
- Bearbeitete Zeit: 17. Januar 2022, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9SSMInstanceProfile

Beschreibung: Diese Richtlinie wird verwendet, um einer Rolle eine Rolle zuzuweisen InstanceProfile , sodass Cloud9 den SSM Session Manager verwenden kann, um eine Verbindung zur Instanz herzustellen

`AWSCloud9SSMInstanceProfile`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloud9SSMInstanceProfile` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Mai 2020, 11:40 UTC
- Bearbeitete Zeit: 14. Mai 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9User

Beschreibung: Erlaubt die Erlaubnis, AWS Cloud9-Entwicklungsumgebungen zu erstellen und eigene Umgebungen zu verwalten.

`AWSCloud9User`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloud9User` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:16 UTC
- Bearbeitete Zeit: 11. Oktober 2023, 13:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:CreateEnvironmentEC2",
        "cloud9:CreateEnvironmentSSH"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:OwnerArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserPublicKey"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
```

```
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudFormationFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CloudFormation.

`AWSCloudFormationFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudFormationFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 26. Juli 2019, 21:50 Uhr UTC
- Bearbeitete Zeit: 26. Juli 2019, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudFormationReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf AWS CloudFormation über die AWS Management Console.

`AWSCloudFormationReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudFormationReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 13. November 2019, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudFrontLogger

Beschreibung: Gewährt CloudFront Logger Schreibberechtigungen für CloudWatch Logs.

`AWSCloudFrontLogger`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juni 2018, 20:15 Uhr UTC
- Bearbeitete Zeit: 22. November 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudHSMFullAccess

Beschreibung: Bietet vollen Zugriff auf alle CloudHSM-Ressourcen.

`AWSCloudHSMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudHSMFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudHSMReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle CloudHSM-Ressourcen.

`AWSCloudHSMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudHSMReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Get*",
        "cloudhsm:List*",
        "cloudhsm:Describe*"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudHSMRole

Beschreibung: Standardrichtlinie für die AWS CloudHSM-Servicerolle.

`AWSCloudHSMRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudHSMRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapDiscoverInstanceAccess

Beschreibung: Bietet Zugriff auf die AWS Cloud Map Discovery API.

`AWSCloudMapDiscoverInstanceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudMapDiscoverInstanceAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2018, 00:02 Uhr UTC
- Bearbeitete Zeit: 20. September 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapFullAccess

Beschreibung: Bietet vollen Zugriff auf alle AWS Cloud Kartenaktionen.

`AWSCloudMapFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudMapFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 23:57 UTC
- Bearbeitete Zeit: 29. Juli 2020, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle AWS Cloud Map-Aktionen.

`AWSCloudMapReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudMapReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 23:45 Uhr UTC
- Bearbeitete Zeit: 20. September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapRegisterInstanceAccess

Beschreibung: Bietet Zugriff auf Registrantenebene auf AWS Cloud Map-Aktionen.

`AWSCloudMapRegisterInstanceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudMapRegisterInstanceAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2018, 00:04 Uhr UTC
- Bearbeitete Zeit: 20. September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudShellFullAccess

Beschreibung: Ermöglicht die Nutzung AWS CloudShell mit allen Funktionen

`AWSCloudShellFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudShellFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 18:07 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudTrail_FullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CloudTrail.

`AWSCloudTrail_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudTrail_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Oktober 2020, 23:41 UTC
- Bearbeitete Zeit: 22. Februar 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudTrail_ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CloudTrail.

`AWSCloudTrail_ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCloudTrail_ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Juni 2022, 17:19 UTC
- Bearbeitete Zeit: 14. Juni 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Beschreibung: Diese Richtlinie wird von der mit dem Dienst verknüpften Rolle mit dem Namen AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents verwendet. CloudWatch verwendet diese dienstbezogene Rolle, um AWS System Manager Incident Manager-Aktionen auszuführen, wenn ein CloudWatch Alarm in den ALARM-Status wechselt. Diese Richtlinie erteilt die Erlaubnis, Incidents in Ihrem Namen zu starten.

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. April 2021, 13:30 Uhr UTC
- Bearbeitete Zeit: 27. April 2021, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeArtifactAdminAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodeArtifact über die AWS Management Console.

`AWSCodeArtifactAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeArtifactAdminAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 16. Juni 2020, 23:53 UTC
- Bearbeitete Zeit: 16. Juni 2020, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeArtifactReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CodeArtifact über die AWS Management Console.

`AWSCodeArtifactReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeArtifactReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juni 2020, 21:23 Uhr UTC
- Bearbeitete Zeit: 25. Juni 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeBuildAdminAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodeBuild über die AWS Management Console. Fügen Sie außerdem AmazonS3 hinzuReadOnlyAccess , um Zugriff auf Download-Build-Artefakte zu gewähren, und fügen Sie IAM hinzu, FullAccess um die Servicerolle für zu erstellen und zu verwalten. CodeBuild

`AWSCodeBuildAdminAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeBuildAdminAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 19:04 UTC
- Bearbeitete Zeit: 2. Mai 2024, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
```

```
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
```

```
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeBuildDeveloperAccess

Beschreibung: Ermöglicht den Zugriff auf AWS CodeBuild über AWS Management Console, ermöglicht jedoch keine CodeBuild Projektverwaltung. Fügen Sie außerdem AmazonS3 hinzuReadOnlyAccess , um Zugriff auf Download-Build-Artefakte zu gewähren.

`AWSCodeBuildDeveloperAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeBuildDeveloperAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 19:02 UTC
- Bearbeitete Zeit: 2. Mai 2024, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
```

```
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
```

```
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeBuildReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CodeBuild über die AWS Management Console. Fügen Sie außerdem AmazonS3 hinzuReadOnlyAccess , um Zugriff auf Download-Build-Artefakte zu gewähren.

`AWSCodeBuildReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeBuildReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 19:03 UTC
- Bearbeitete Zeit: 2. Mai 2024, 01:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
```

```
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codebuild:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeCommitFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodeCommit über die AWS Management Console.

`AWSCodeCommitFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeCommitFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:02 UTC
- Bearbeitete Zeit: 17. Juli 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
```

```
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeCommitPowerUser

Beschreibung: Bietet vollen Zugriff auf AWS CodeCommit Repositorys, erlaubt aber nicht das Löschen von Repositorys.

`AWSCodeCommitPowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeCommitPowerUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:06 UTC
- Bearbeitete Zeit: 17. Juli 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
```

```
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
```

```
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
```

```
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
```

```
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeCommitReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CodeCommit über die AWS Management Console.

`AWSCodeCommitReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeCommitReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:05 UTC
- Bearbeitete Zeit: 18. August 2021, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials",
        "iam:ListAccessKeys",
        "iam:GetSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codecommit:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployDeployerAccess

Beschreibung: Ermöglicht den Zugriff auf die Registrierung und Bereitstellung einer Revision.

`AWSCodeDeployDeployerAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeDeployDeployerAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Mai 2015, 18:18 Uhr UTC
- Bearbeitete Zeit: 2. April 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployFullAccess

Beschreibung: Bietet vollen Zugriff auf CodeDeploy Ressourcen.

`AWSCodeDeployFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeDeployFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Mai 2015, 18:13 Uhr UTC
- Bearbeitete Zeit: 2. April 2020, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CodeDeploy Ressourcen.

`AWSCodeDeployReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeDeployReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Mai 2015, 18:21 Uhr UTC
- Bearbeitete Zeit: 2. April 2020, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codedeploy:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRole

Beschreibung: Bietet CodeDeploy Servicezugriff, um Tags zu erweitern und in Ihrem Namen mit Auto Scaling zu interagieren.

`AWSCodeDeployRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeDeployRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. Mai 2015, 18:05 Uhr UTC
- Bearbeitete Zeit: 16. August 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForCloudFormation

Beschreibung: Bietet CodeDeploy Servicezugriff zum Aufrufen der Lambda-Funktion in Ihrem Namen, um eine Blue/Green-Bereitstellung durchzuführen. CloudFormation

`AWSCodeDeployRoleForCloudFormation`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeDeployRoleForCloudFormation` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. Mai 2020, 17:12 Uhr UTC
- Bearbeitete Zeit: 19. Mai 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForECS

Beschreibung: Bietet CodeDeploy serviceweiten Zugriff, sodass Sie in Ihrem Namen eine ECS Blue/Green-Implementierung durchführen können. Gewährt vollen Zugriff auf Support-Services, z. B. vollen Zugriff zum Lesen aller S3-Objekte, zum Aufrufen aller Lambda-Funktionen, zum Veröffentlichen zu allen SNS-Themen innerhalb des Kontos und zum Aktualisieren aller ECS-Services.

`AWSCodeDeployRoleForECS`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeDeployRoleForECS` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 20:40 UTC
- Bearbeitete Zeit: 23. September 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForECSLimited

Beschreibung: Bietet eingeschränkten Zugriff auf den CodeDeploy Service, sodass Sie in Ihrem Namen eine ECS Blue/Green-Implementierung durchführen können.

`AWSCodeDeployRoleForECSLimited`dist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeDeployRoleForECSLimited` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 20:42 UTC
- Bearbeitete Zeit: 23. September 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForLambda

Beschreibung: Bietet CodeDeploy Servicezugriff, um eine Lambda-Bereitstellung in Ihrem Namen durchzuführen.

`AWSCodeDeployRoleForLambda`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeDeployRoleForLambda` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 28. November 2017, 14:05 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForLambdaLimited

Beschreibung: Bietet eingeschränkten CodeDeploy Dienstzugriff zur Durchführung einer Lambda-Bereitstellung in Ihrem Namen.

`AWSCodeDeployRoleForLambdaLimited`dist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeDeployRoleForLambdaLimited` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. August 2020, 17:14 Uhr UTC
- Bearbeitete Zeit: 17. August 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodePipeline_FullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodePipeline über die AWS Management Console.

`AWSCodePipeline_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodePipeline_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. August 2020, 22:38 UTC
- Bearbeitete Zeit: 14. März 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodePipeline_ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CodePipeline über die AWS Management Console.

`AWSCodePipeline_ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodePipeline_ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. August 2020, 22:25 Uhr UTC
- Bearbeitete Zeit: 3. August 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodePipelineApproverAccess

Beschreibung: Ermöglicht den Zugriff auf das Anzeigen und Genehmigen manueller Änderungen für alle Pipelines

`AWSCodePipelineApproverAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodePipelineApproverAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Juli 2016, 18:59 Uhr UTC
- Bearbeitete Zeit: 2. August 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodePipelineCustomActionAccess

Beschreibung: Ermöglicht den Zugriff auf benutzerdefinierte Aktionen zum Abrufen von Auftragsdetails (einschließlich temporärer Anmeldeinformationen) und zum Melden von Statusaktualisierungen AWS CodePipeline.

`AWSCodePipelineCustomActionAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodePipelineCustomActionAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:02 UTC

- Bearbeitete Zeit: 9. Juli 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeStarFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodeStar über die AWS Management Console.

`AWSCodeStarFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeStarFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. April 2017, 16:23 UTC
- Bearbeitete Zeit: 28. März 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeStarNotificationsServiceRolePolicy

Beschreibung: Ermöglicht AWS CodeStar Notifications den Zugriff auf Amazon CloudWatch Events in Ihrem Namen

`AWSCodeStarNotificationsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. November 2019, 16:10 UTC
- Bearbeitete Zeit: 19. März 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeStarServiceRole

Beschreibung: NICHT VERWENDEN — AWS CodeStar Service Role Policy, die Administratorrechte für CodeStar die Verwaltung von IAM und anderen Serviceressourcen im Namen des Kunden gewährt.

`AWSCodeStarServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCodeStarServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. April 2017, 15:20 Uhr UTC
- Bearbeitete Zeit: 20. September 2021, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCompromisedKeyQuarantine

Beschreibung: Verweigert den Zugriff auf bestimmte Aktionen, die vom AWS Team angewendet werden, falls die Anmeldeinformationen eines IAM-Benutzers kompromittiert oder öffentlich zugänglich gemacht wurden. Entfernen Sie diese Richtlinie NICHT. Folgen Sie stattdessen den Anweisungen in der E-Mail, die Sie zu dieser Veranstaltung erhalten haben.

`AWSCompromisedKeyQuarantine`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCompromisedKeyQuarantine` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. August 2020, 18:04 UTC

- Bearbeitete Zeit: 11. August 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCompromisedKeyQuarantineV2

Beschreibung: Verweigert den Zugriff auf bestimmte Aktionen, die vom AWS Team angewendet werden, falls die Anmeldeinformationen eines IAM-Benutzers kompromittiert oder öffentlich zugänglich gemacht wurden. Entfernen Sie diese Richtlinie NICHT. Folgen Sie stattdessen den Anweisungen in der für Sie erstellten Support-Anfrage zu dieser Veranstaltung.

`AWSCompromisedKeyQuarantineV2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCompromisedKeyQuarantineV2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. April 2021, 22:30 Uhr UTC
- Bearbeitete Zeit: 16. März 2023, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
```

```
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigMultiAccountSetupPolicy

Beschreibung: Ermöglicht Config, AWS Dienste aufzurufen und Konfigurationsressourcen unternehmensweit bereitzustellen

`AWSConfigMultiAccountSetupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Juni 2019, 18:03 UTC
- Bearbeitete Zeit: 24. Februar 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigRemediationServiceRolePolicy

Beschreibung: Ermöglicht AWS Config, nicht konforme Ressourcen in Ihrem Namen zu korrigieren.

`AWSConfigRemediationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. Juni 2019, 21:21 Uhr UTC
- Bearbeitete Zeit: 18. Juni 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigRoleForOrganizations

Beschreibung: Ermöglicht AWS Config, schreibgeschützte AWS Organisations-APIs aufzurufen

`AWSConfigRoleForOrganizations`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSConfigRoleForOrganizations` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. März 2018, 22:53 Uhr UTC
- Zeit bearbeitet: 24. November 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigRulesExecutionRole

Beschreibung: Ermöglicht einer AWS Lambda-Funktion den Zugriff auf die AWS Config-API und die Konfigurations-Snapshots, die AWS Config regelmäßig an Amazon S3 übermittelt. Dieser Zugriff ist für Funktionen erforderlich, die Konfigurationsänderungen für benutzerdefinierte Konfigurationsregeln auswerten.

`AWSConfigRulesExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSConfigRulesExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. März 2016, 17:59 Uhr UTC
- Bearbeitete Zeit: 13. Mai 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigServiceRolePolicy

Beschreibung: Ermöglicht Config, in Ihrem Namen AWS Dienste aufzurufen und Ressourcenkonfigurationen zu sammeln.

`AWSConfigServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. Mai 2018, 23:31 UTC
- Bearbeitete Zeit: 22. Februar 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v50 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
```

```
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListThemes",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
```

```
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
```

```
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:GetAnomalyMonitors",
```

```
        "ce:GetAnomalySubscriptions",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListTypes",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeRepository",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
```

```
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePrompt",
        "connect:DescribeQuickConnect",
        "connect:DescribeRule",
```

```
        "connect:DescribeUser",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQuickConnects",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
```

```
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "detective:ListGraphs",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:DescribeClientVpnAuthorizationRules",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeDhcpOptions",
```

```
        "ec2:DescribeFleets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
```

```
        "eks:DescribeNodegroup",
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
```

```
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
```

```
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
```

```
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSecurityConfiguration",
```

```
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
```

```
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
```

```
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
```

```
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
```

```
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:ListConnectors",
```

```
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
```

```
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:GetDataProtectionPolicy",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
```

```
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeFlow",
        "mediaconnect:ListFlows",
        "mediaconnect:ListTagsForResource",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
```

```
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
```

```
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
```

```
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
```

```
            "redshift:DescribeEndpointAccess",
            "redshift:DescribeEndpointAuthorization",
            "redshift:DescribeEventSubscriptions",
            "redshift:DescribeLoggingStatus",
            "redshift:DescribeScheduledActions",
            "refactor-spaces:GetEnvironment",
            "refactor-spaces:GetService",
            "refactor-spaces:ListApplications",
            "refactor-spaces:ListEnvironments",
            "refactor-spaces:ListServices",
            "rekognition:DescribeStreamProcessor",
            "rekognition:ListStreamProcessors",
            "rekognition:ListTagsForResource",
            "resiliencehub:DescribeApp",
            "resiliencehub:DescribeAppVersionTemplate",
            "resiliencehub:DescribeResiliencyPolicy",
            "resiliencehub:ListApps",
            "resiliencehub:ListAppVersionResourceMappings",
            "resiliencehub:ListResiliencyPolicies",
            "resiliencehub:ListTagsForResource",
            "resource-explorer-2:GetIndex",
            "resource-explorer-2:ListIndexes",
            "resource-explorer-2:ListTagsForResource",
            "resource-groups:GetGroup",
            "resource-groups:GetGroupConfiguration",
            "resource-groups:GetGroupQuery",
            "resource-groups:GetTags",
            "resource-groups:ListGroupResources",
            "resource-groups:ListGroups",
            "robomaker:DescribeRobotApplication",
            "robomaker:DescribeSimulationApplication",
            "robomaker:ListRobotApplications",
            "robomaker:ListSimulationApplications",
            "route53-recovery-control-config:DescribeCluster",
            "route53-recovery-control-config:DescribeControlPanel",
            "route53-recovery-control-config:DescribeRoutingControl",
            "route53-recovery-control-config:DescribeSafetyRule",
            "route53-recovery-control-config:ListClusters",
            "route53-recovery-control-config:ListControlPanels",
            "route53-recovery-control-config:ListRoutingControls",
            "route53-recovery-control-config:ListSafetyRules",
            "route53-recovery-control-config:ListTagsForResource",
            "route53-recovery-readiness:GetCell",
            "route53-recovery-readiness:GetReadinessCheck",
```

```
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
```

```
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
```

```
        "s3:ListStorageLensConfigurations",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeWorkteam",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
```

```
            "sagemaker:ListTags",
            "sagemaker:ListWorkteams",
            "schemas:DescribeDiscoverer",
            "schemas:DescribeRegistry",
            "schemas:DescribeSchema",
            "schemas:GetResourcePolicy",
            "schemas:ListDiscoverers",
            "schemas:ListRegistries",
            "schemas:ListSchemas",
            "sdb:GetAttributes",
            "sdb:ListDomains",
            "secretsmanager:ListSecrets",
            "secretsmanager:ListSecretVersionIds",
            "securityhub:DescribeHub",
            "serviceCatalog:DescribePortfolioShares",
            "servicediscovery:GetInstance",
            "servicediscovery:GetNamespace",
            "servicediscovery:GetService",
            "servicediscovery:ListInstances",
            "servicediscovery:ListNamespaces",
            "servicediscovery:ListServices",
            "servicediscovery:ListTagsForResource",
            "ses:DescribeReceiptRule",
            "ses:DescribeReceiptRuleSet",
            "ses:GetConfigurationSet",
            "ses:GetConfigurationSetEventDestinations",
            "ses:GetContactList",
            "ses:GetEmailTemplate",
            "ses:GetTemplate",
            "ses:ListConfigurationSets",
            "ses:ListContactLists",
            "ses:ListEmailTemplates",
            "ses:ListReceiptFilters",
            "ses:ListReceiptRuleSets",
            "ses:ListTemplates",
            "shield:DescribeDRTAccess",
            "shield:DescribeProtection",
            "shield:DescribeSubscription",
            "signer:GetSigningProfile",
            "signer:ListProfilePermissions",
            "signer:ListSigningProfiles",
            "sns:GetDataProtectionPolicy",
            "sns:GetSMSSandboxAccountStatus",
            "sns:GetSubscriptionAttributes",
```

```
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetDocument",
        "ssm:ListDocuments",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:ListActivities",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
```

```
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigUserAccess

Beschreibung: Ermöglicht den Zugriff auf die Verwendung von AWS Config, einschließlich der Suche nach Tags in Ressourcen und dem Lesen aller Tags. Dies gewährt keine Berechtigung zur Konfiguration von AWS Config, wofür Administratorrechte erforderlich sind.

`AWSConfigUserAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSConfigUserAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Februar 2015, 19:38 UTC
- Bearbeitete Zeit: 18. März 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConnector

Beschreibung: Ermöglicht umfassenden Lese-/Schreibzugriff auf ALLE EC2-Objekte, Lese-/Schreibzugriff auf S3-Buckets, die mit „import-to-ec2-“ beginnen, und die Möglichkeit, alle S3-Buckets aufzulisten, damit der Connector VMs in Ihrem Namen importieren kann. AWS

`AWSConnector`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSConnector` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Februar 2015, 17:14 Uhr UTC
- Zeit bearbeitet: 28. September 2015, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSControlTowerAccountServiceRolePolicy

Beschreibung: Ermöglicht AWS Control Tower, AWS Dienste aufzurufen, die eine automatisierte Kontokonfiguration und zentrale Verwaltung in Ihrem Namen bereitstellen.

`AWSControlTowerAccountServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Juni 2023, 22:04 UTC
- Bearbeitete Zeit: 5. Juni 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "events:source" : "aws.securityhub"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com",
          "events:detail-type" : "Security Hub Findings - Imported"
        }
      }
    },
```

```
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
    },
    {
      "Sid" : "AllowControlTowerToPublishSecurityNotifications",
      "Effect" : "Allow",
      "Action" : "sns:publish",
      "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "AllowActionsForSecurityHubIntegration",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards"
      ],
```

```
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSControlTowerServiceRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von AWS Control Tower verwaltet oder verwendet werden

`AWSControlTowerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSControlTowerServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 03. Mai 2019, 18:19 Uhr UTC
- Bearbeitete Zeit: 12. April 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCostAndUsageReportAutomationPolicy

Beschreibung: Erteilt die Berechtigung, die Organisation des Kontos zu beschreiben, S3-Buckets für das MAP-Programm zu erstellen und Tags darauf anzuwenden, einen Kosten- und Nutzungsbericht zu erstellen und Definitionen von Kosten- und Nutzungsberichten zu beschreiben.

`AWSCostAndUsageReportAutomationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSCostAndUsageReportAutomationPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. November 2021, 21:27 UTC
- Bearbeitete Zeit: 1. November 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS Data Exchange und AWS Marketplace Aktionen mithilfe des AWS Management Console SDK. Es bietet auch ausgewählten Zugriff auf verwandte Dienste, die erforderlich sind, um den AWS Data Exchange in vollem Umfang nutzen zu können.

`AWSDataExchangeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataExchangeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 7. Mai 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
```

```
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceProviderActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:GetPrivateListing",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeProviderFullAccess

Beschreibung: Gewährt Datenanbietern Zugriff auf AWS Data Exchange und AWS Marketplace Aktionen mithilfe des SDK AWS Management Console und. Es bietet auch ausgewählten Zugriff auf verwandte Dienste, die erforderlich sind, um den AWS Data Exchange in vollem Umfang nutzen zu können.

`AWSDataExchangeProviderFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataExchangeProviderFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 15. März 2022, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:CreateRevision",
        "dataexchange:CreateAsset",
        "dataexchange:Get*",
        "dataexchange:Update*",
        "dataexchange:List*",
        "dataexchange:Delete*",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "dataexchange:PublishDataSet",
        "dataexchange:SendApiAsset",
        "dataexchange:RevokeRevision",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
```

```
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeReadOnly

Beschreibung: Gewährt schreibgeschützten Zugriff auf AWS Data Exchange und AWS Marketplace Aktionen mithilfe des SDK AWS Management Console und.

`AWSDataExchangeReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataExchangeReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 10. Mai 2021, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeSubscriberFullAccess

Beschreibung: Gewährt Datenabonnenten Zugriff auf AWS Data Exchange und AWS Marketplace Aktionen mithilfe des SDK AWS Management Console und. Es bietet auch ausgewählten Zugriff auf verwandte Dienste, die erforderlich sind, um den AWS Data Exchange in vollem Umfang nutzen zu können.

`AWSDataExchangeSubscriberFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataExchangeSubscriberFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 21. Mai 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataLifecycleManagerServiceRole

Beschreibung: Stellt AWS Data Lifecycle Manager die entsprechenden Berechtigungen zur Verfügung, um Aktionen mit AWS Ressourcen zu ergreifen

`AWSDataLifecycleManagerServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataLifecycleManagerServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Juli 2018, 19:34 UTC
- Bearbeitete Zeit: 19. September 2022, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
```

```
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataLifecycleManagerServiceRoleForAMIManagement

Beschreibung: Stellt AWS Data Lifecycle Manager die entsprechenden Berechtigungen zur Verfügung, um Aktionen an AWS Ressourcen für AMI Management durchzuführen

`AWSDataLifecycleManagerServiceRoleForAMIManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataLifecycleManagerServiceRoleForAMIManagement` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 21. Oktober 2020, 19:39 UTC
- Bearbeitete Zeit: 19. August 2021, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataLifecycleManagerSSMFullAccess

Beschreibung: Erlaubt Amazon Data Lifecycle Manager die Erlaubnis, die Systems Manager Manager-Aktionen auszuführen, die für die Ausführung von Pre- und Post-Skripten auf allen Amazon EC2 EC2-Instances erforderlich sind.

`AWSDataLifecycleManagerSSMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataLifecycleManagerSSMFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 31. Oktober 2023, 20:29 UTC
- Bearbeitete Zeit: 16. November 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataPipeline_FullAccess

Beschreibung: Bietet vollen Zugriff auf Data Pipeline, Listenzugriff für S3-, DynamoDB-, Redshift-, RDS-, SNS- und IAM-Rollen sowie PassRole-Zugriff für Standardrollen.

`AWSDataPipeline_FullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataPipeline_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Januar 2017, 23:14 Uhr UTC
- Bearbeitete Zeit: 17. August 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataPipeline_PowerUser

Beschreibung: Bietet vollen Zugriff auf Data Pipeline, Listenzugriff für S3-, DynamoDB-, Redshift-, RDS-, SNS- und IAM-Rollen sowie PassRole-Zugriff für Standardrollen.

`AWSDataPipeline_PowerUser`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataPipeline_PowerUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Januar 2017, 23:16 UTC
- Zeit bearbeitet: 17. August 2017, 18:49 UTC

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

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataSyncDiscoveryServiceRolePolicy

Beschreibung: Ermöglicht DataSync Discovery die Integration mit anderen AWS Diensten in Ihrem Namen.

`AWSDataSyncDiscoveryServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. März 2023, 22:19 UTC
- Bearbeitete Zeit: 20. März 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataSyncFullAccess

Beschreibung: Bietet vollen AWS DataSync und minimalen Zugriff auf die zugehörigen Abhängigkeiten

`AWSDataSyncFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataSyncFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2019, 19:40 Uhr UTC
- Bearbeitete Zeit: 16. Februar 2024, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "outposts:ListOutposts",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListRegionalBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataSyncPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datasync.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataSyncReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS DataSync

`AWSDataSyncReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDataSyncReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2019, 19:18 UTC
- Bearbeitete Zeit: 30. Juni 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-FleetWorker

Beschreibung: Ermöglicht Mitarbeitern von AWS Deadline Cloud den Zugriff auf die Ausführung von Aufgaben auf einer Farm.

`AWSDeadlineCloud-FleetWorker`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeadlineCloud-FleetWorker` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:21 UTC
- Bearbeitete Zeit: 1. April 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-UserAccessFarms

Beschreibung: Ermöglicht Benutzern Workstation-Zugriff auf AWS Deadline Cloud-Farmen mit eingeschränkten Leseberechtigungen, um andere erforderliche Dienste aufzurufen. Ordnen Sie diese Richtlinie der Benutzerrolle zu, die Ihrem Studio zugeordnet ist.

`AWSDeadlineCloud-UserAccessFarms`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeadlineCloud-UserAccessFarms` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 16:54 UTC
- Bearbeitete Zeit: 1. April 2024, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:CreateBudget",
        "deadline:DeleteBudget",
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue",
        "deadline:GetBudget",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:ListBudgets",
        "deadline:StartSessionsStatisticsAggregation",
        "deadline:UpdateBudget"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
```

```
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFarm",
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
```

```
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarmMembers",
        "deadline:ListFleetMembers",
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetWorker",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
```

```
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-UserAccessFleets

Beschreibung: Ermöglicht Benutzern den Workstation-Zugriff auf AWS Deadline Cloud-Flotten mit eingeschränkten Leseberechtigungen, um andere erforderliche Dienste aufzurufen. Ordnen Sie diese Richtlinie der Benutzerrolle zu, die Ihrem Studio zugeordnet ist.

`AWSDeadlineCloud-UserAccessFleets`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeadlineCloud-UserAccessFleets` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:01 UTC
- Bearbeitete Zeit: 1. April 2024, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-UserAccessJobs

Beschreibung: Ermöglicht Benutzern Workstation-Zugriff auf AWS Deadline Cloud-Jobs mit eingeschränkten Leseberechtigungen zum Aufrufen anderer erforderlicher Dienste. Ordnen Sie diese Richtlinie der Benutzerrolle zu, die Ihrem Studio zugeordnet ist.

`AWSDeadlineCloud-UserAccessJobs`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeadlineCloud-UserAccessJobs` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:05 UTC

- Bearbeitete Zeit: 1. April 2024, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "deadline:GetJob",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetTask",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListTasks",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-UserAccessQueues

Beschreibung: Ermöglicht Benutzerarbeitsstationen den Zugriff auf AWS Deadline Cloud-Warteschlangen mit eingeschränkten Leseberechtigungen zum Aufrufen anderer erforderlicher Dienste. Ordnen Sie diese Richtlinie der Benutzerrolle zu, die Ihrem Studio zugeordnet ist.

`AWSDeadlineCloud-UserAccessQueues`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeadlineCloud-UserAccessQueues` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:10 UTC
- Bearbeitete Zeit: 1. April 2024, 17:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetJob",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-WorkerHost

Beschreibung: Ermöglicht AWS Deadline Cloud-Worker-Hosts den Zugriff, um einer Flotte in einer Farm beizutreten.

`AWSDeadlineCloud-WorkerHost`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeadlineCloud-WorkerHost` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:28 UTC
- Bearbeitete Zeit: 1. April 2024, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
```

```
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepLensLambdaFunctionAccessPolicy

Beschreibung: Diese Richtlinie legt die Berechtigungen fest, die für DeepLens administrative Lambda-Funktionen erforderlich sind, die auf einem DeepLens Gerät ausgeführt werden

`AWSDeepLensLambdaFunctionAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeepLensLambdaFunctionAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 15:47 Uhr UTC
- Bearbeitete Zeit: 11. Juni 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepLensServiceRolePolicy

Beschreibung: Gewährt AWS DeepLens Zugriff auf Ressourcen und Rollen AWS-Services, die von DeepLens und seinen Abhängigkeiten benötigt werden, einschließlich IoT, S3 GreenGrass und AWS Lambda.

`AWSDeepLensServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeepLensServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. November 2017, 15:46 Uhr UTC
- Bearbeitete Zeit: 25. September 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerAccountAdminAccess

Beschreibung: DeepRacer Administratorzugriff auf alle Aktionen, einschließlich des Umschaltens zwischen Mehrbenutzer- und Einzelbenutzermodus.

`AWSDeepRacerAccountAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeepRacerAccountAdminAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Oktober 2021, 01:27 UTC
- Bearbeitete Zeit: 28. Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerCloudFormationAccessPolicy

Beschreibung: Ermöglicht CloudFormation das Erstellen und Verwalten von AWS Stacks und Ressourcen in Ihrem Namen.

`AWSDeepRacerCloudFormationAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeepRacerCloudFormationAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Februar 2019, 21:59 UTC
- Bearbeitete Zeit: 14. Juni 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerDefaultMultiUserAccess

Beschreibung: DeepRacer MultiUser Standardbenutzerzugriff zur Verwendung von Deepracer im Mehrbenutzermodus

`AWSDeepRacerDefaultMultiUserAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeepRacerDefaultMultiUserAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Oktober 2021, 01:27 UTC
- Bearbeitete Zeit: 28. Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS DeepRacer. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3).

`AWSDeepRacerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeepRacerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Oktober 2020, 22:03 UTC
- Bearbeitete Zeit: 5. Oktober 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerRoboMakerAccessPolicy

Beschreibung: Ermöglicht RoboMaker das Erstellen der erforderlichen Ressourcen und das Anrufen von AWS Diensten in Ihrem Namen.

`AWSDeepRacerRoboMakerAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeepRacerRoboMakerAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Februar 2019, 21:59 UTC
- Bearbeitete Zeit: 28. Februar 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerServiceRolePolicy

Beschreibung: Ermöglicht DeepRacer das Erstellen der erforderlichen Ressourcen und das Anrufen von AWS Diensten in Ihrem Namen.

`AWSDeepRacerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeepRacerServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 28. Februar 2019, 21:58 Uhr UTC
- Bearbeitete Zeit: 12. Juni 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDenyAll

Beschreibung: Jeglichen Zugriff verweigern.

`AWSDenyAll`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDenyAll` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Mai 2019, 22:36 UTC
- Bearbeitete Zeit: 18. Dezember 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeviceFarmFullAccess

Beschreibung: Bietet vollen Zugriff auf alle AWS Device Farm Farm-Operationen.

`AWSDeviceFarmFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDeviceFarmFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 13. Juli 2015, 16:37 UTC
- Zeit bearbeitet: 13. Juli 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeviceFarmServiceRolePolicy

Beschreibung: Erteilen Sie AWS Device Farm die Erlaubnis, EC2-Netzwerk-APIs in Ihrem Namen aufzurufen.

`AWSDeviceFarmServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. September 2022, 21:02 UTC
- Bearbeitete Zeit: 20. September 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeviceFarmTestGridServiceRolePolicy

Beschreibung: Erteilen Sie AWS Device Farm die Erlaubnis, EC2-APIs in Ihrem Namen aufzurufen.

`AWSDeviceFarmTestGridServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. Mai 2021, 22:01 UTC
- Bearbeitete Zeit: 26. Mai 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectConnectFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Direct Connect über die AWS Management Console.

`AWSDirectConnectFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDirectConnectFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 30. April 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectConnectReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Direct Connect über die AWS Management Console.

`AWSDirectConnectReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDirectConnectReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 18. Mai 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectConnectServiceRolePolicy

Beschreibung: AWS Erlaubt Direct Connect, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

`AWSDirectConnectServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. Januar 2021, 18:35 UTC
- Bearbeitete Zeit: 14. Januar 2021, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectoryServiceFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Directory Service.

`AWSDirectoryServiceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDirectoryServiceFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 02. April 2024, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectoryServiceReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den AWS Directory Service.

`AWSDirectoryServiceReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDirectoryServiceReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 25. September 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDiscoveryContinuousExportFirehosePolicy

Beschreibung: Bietet Schreibzugriff auf AWS Ressourcen, die für AWS Discovery Continuous Export erforderlich sind

`AWSDiscoveryContinuousExportFirehosePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSDiscoveryContinuousExportFirehosePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 9. August 2018, 18:29 Uhr UTC
- Bearbeitete Zeit: 8. Juni 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDMSFleetAdvisorServiceRolePolicy

Beschreibung: Ermöglicht DMS Fleet Advisor, CloudWatch Metriken in Ihrem Namen zu verwalten.

`AWSDMSFleetAdvisorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. März 2023, 09:10 UTC
- Bearbeitete Zeit: 6. März 2023, 09:10 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDMSServerlessServiceRolePolicy

Beschreibung: Erteilt AWS DMS Serverless die Berechtigung, in Ihrem Namen DMS-Ressourcen in Ihrem Konto zu erstellen und zu verwalten

`AWSDMSServerlessServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. Mai 2023, 20:28 UTC
- Bearbeitete Zeit: 18. Mai 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:DeleteReplicationInstance"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id3",
      "Effect" : "Allow",
      "Action" : [
        "dms:TestConnection",
        "dms:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:endpoint:*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2CapacityReservationFleetRolePolicy

Beschreibung: Ermöglicht dem EC2 CapacityReservation Fleet Service die Verwaltung von Kapazitätsreservierungen

`AWSEC2CapacityReservationFleetRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. September 2021, 14:43 UTC
- Bearbeitete Zeit: 29. September 2021, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:CapacityReservationFleet" : "arn:aws:ec2:*:*:capacity-reservation-fleet/
crf-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CreateCapacityReservation"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2FleetServiceRolePolicy

Beschreibung: Ermöglicht EC2 Fleet das Starten und Verwalten von Instances.

`AWSEC2FleetServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. März 2018, 00:08 Uhr UTC
- Bearbeitete Zeit: 4. Mai 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2SpotFleetServiceRolePolicy

Beschreibung: Ermöglicht EC2 Spot Fleet den Start und die Verwaltung von Spot-Flotteninstanzen

`AWSEC2SpotFleetServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. Oktober 2017, 19:13 Uhr UTC
- Bearbeitete Zeit: 16. März 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2SpotServiceRolePolicy

Beschreibung: Ermöglicht EC2 Spot das Starten und Verwalten von Spot-Instances

`AWSEC2SpotServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. September 2017, 18:51 Uhr UTC
- Bearbeitete Zeit: 12. Dezember 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2VssSnapshotPolicy

Beschreibung: Diese Richtlinie ist an die IAM-Rolle angehängt, die Ihren Amazon EC2-Windows-Instances zugewiesen ist, damit die Amazon EC2 VSS-Lösung Tags erstellen und Amazon Machine Images (AMI) und EBS-Snapshots hinzufügen kann.

`AWSEC2VssSnapshotPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSEC2VssSnapshotPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. März 2024, 16:32 UTC
- Bearbeitete Zeit: 27. März 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceInfo",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:SourceInstanceARN" : "*${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
```

```
    },
    {
      "Sid" : "CreateSnapshotsAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:SourceInstanceARN" : "*${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "CreateImageWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateImageAccessInstance",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:SourceInstanceARN" : "*${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateImage",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsAfterResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "AppConsistent",
            "Device"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeImagesAndSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSECRPullThroughCache_ServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Dienste und Ressourcen, die vom AWS ECR-Pull-Through-Cache verwendet oder verwaltet werden

`AWSECRPullThroughCache_ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2021, 21:51 UTC
- Bearbeitete Zeit: 13. November 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkCustomPlatformforEC2Role

Beschreibung: Erteilen Sie der Instance in Ihrer benutzerdefinierten Platform Builder-Umgebung die Erlaubnis, eine EC2-Instance zu starten, EBS-Snapshot und AMI zu erstellen, Logs an Amazon CloudWatch Logs zu streamen und Artefakte in Amazon S3 zu speichern.

`AWSElasticBeanstalkCustomPlatformforEC2Role`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkCustomPlatformforEC2Role` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Februar 2017, 22:50 UTC
- Zeit bearbeitet: 21. Februar 2017, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkEnhancedHealth

Beschreibung: AWS Elastic Beanstalk Service-Richtlinie für das Gesundheitsüberwachungssystem

`AWSElasticBeanstalkEnhancedHealth`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkEnhancedHealth` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Februar 2016, 23:17 UTC
- Bearbeitete Zeit: 9. April 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkMaintenance

Beschreibung: AWS Elastic Beanstalk Service Role Policy, die eingeschränkte Berechtigungen zur Aktualisierung Ihrer Ressourcen in Ihrem Namen zu Wartungszwecken gewährt.

`AWSElasticBeanstalkMaintenance`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 11. Januar 2019, 23:22 UTC
- Bearbeitete Zeit: 29. April 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Beschreibung: Diese Richtlinie gilt für die AWS Elastic Beanstalk-Servicerolle, die zur Durchführung verwalteter Updates von Elastic Beanstalk Beanstalk-Umgebungen verwendet wird. Diese Richtlinie sollte nicht mit anderen Benutzern oder Rollen verknüpft werden. Die Richtlinie gewährt umfassende Berechtigungen zum Erstellen und Verwalten von Ressourcen für eine Reihe von AWS Diensten AutoScaling, darunter EC2, ECS, Elastic Load Balancing und CloudFormation. Diese Richtlinie ermöglicht auch die Weitergabe jeder IAM-Rolle, die mit diesen Diensten verwendet werden kann.

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. März 2021, 22:18 Uhr UTC
- Bearbeitete Zeit: 23. März 2023, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Beschreibung: AWS Elastic Beanstalk Service Role-Richtlinie, die eingeschränkte Berechtigungen für verwaltete Updates gewährt.

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. November 2019, 22:35 Uhr UTC
- Bearbeitete Zeit: 29. April 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElasticBeanstalkAPIs",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
```

```
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
```

```
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
    },
    {
      "Sid" : "EC2LaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*"
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
```

```
        }
      }
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkMulticontainerDocker

Beschreibung: Stellen Sie den Instances in Ihrer Docker-Umgebung mit mehreren Containern Zugriff bereit, um den Amazon EC2 Container Service zur Verwaltung von Container-Bereitstellungsaufgaben zu verwenden.

`AWSElasticBeanstalkMulticontainerDocker`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkMulticontainerDocker` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Februar 2016, 23:15 UTC
- Bearbeitete Zeit: 23. März 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkReadOnly

Beschreibung: Gewährt nur Leseberechtigungen. Ermöglicht Betreibern ausdrücklich den direkten Zugriff auf Informationen über Ressourcen im Zusammenhang mit AWS Elastic Beanstalk Beanstalk-Anwendungen.

`AWSElasticBeanstalkReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. Januar 2021, 19:02 UTC
- Bearbeitete Zeit: 22. Januar 2021, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleCore

Beschreibung: AWSElasticBeanstalkRoleCore (Rolle „Elastic Beanstalk Operations“) Ermöglicht den Kernbetrieb einer Webservice-Umgebung.

`AWSElasticBeanstalkRoleCore`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkRoleCore` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:48 UTC
- Bearbeitete Zeit: 30. April 2024, 00:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleCWL

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Umgebung die Verwaltung von Amazon CloudWatch Logs-Protokollgruppen.

`AWSElasticBeanstalkRoleCWL`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkRoleCWL` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:49 UTC

- Bearbeitete Zeit: 5. Juni 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleECS

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Docker-Umgebung mit mehreren Containern die Verwaltung von Amazon ECS-Clustern.

`AWSElasticBeanstalkRoleECS`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkRoleECS` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:47 UTC
- Bearbeitete Zeit: 23. März 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleRDS

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Umgebung die Integration einer Amazon RDS-Instance.

`AWSElasticBeanstalkRoleRDS`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkRoleRDS` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:46 UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleSNS

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Umgebung, die Amazon SNS SNS-Themenintegration zu ermöglichen.

`AWSElasticBeanstalkRoleSNS`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkRoleSNS` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:46 UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleWorkerTier

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Worker-Umgebungsebene, eine Amazon DynamoDB-Tabelle und eine Amazon SQS SQS-Warteschlange zu erstellen.

`AWSElasticBeanstalkRoleWorkerTier`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkRoleWorkerTier` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:43 UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkService

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/iam-servicerole.html. AWS Elastic Beanstalk Service-Rollenrichtlinie, die Berechtigungen zum Erstellen und Verwalten von Ressourcen (d. h.: AutoScaling EC2, S3 CloudFormation, ELB usw.) in Ihrem Namen gewährt.

`AWSElasticBeanstalkService`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkService` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. April 2016, 20:27 UTC
- Bearbeitete Zeit: 10. Mai 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Version der Richtlinie

Richtlinienversion: v17 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkServiceRolePolicy

Beschreibung: AWS Elastic Beanstalk Service Linked Role-Richtlinie, die Berechtigungen zum Erstellen und Verwalten von Ressourcen (d. h.: AutoScaling EC2, S3 CloudFormation, ELB usw.) in Ihrem Namen gewährt.

`AWSElasticBeanstalkServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. September 2017, 23:46 Uhr UTC
- Bearbeitete Zeit: 6. Juni 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkWebTier

Beschreibung: Geben Sie den Instances in Ihrer Webserver-Umgebung Zugriff, um Protokolldateien auf Amazon S3 hochzuladen.

`AWSElasticBeanstalkWebTier`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkWebTier` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Februar 2016, 23:08 UTC
- Bearbeitete Zeit: 9. September 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkWorkerTier

Beschreibung: Geben Sie den Instances in Ihrer Arbeitsumgebung Zugriff, um Protokolldateien auf Amazon S3 hochzuladen, Amazon SQS zur Überwachung der Job-Warteschlange Ihrer Anwendung zu verwenden, Amazon DynamoDB für die Auswahl von Führungskräften zu verwenden und für Amazon, um Metriken für die Zustandsüberwachung CloudWatch zu veröffentlichen.

`AWSElasticBeanstalkWorkerTier`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticBeanstalkWorkerTier` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Februar 2016, 23:12 UTC
- Zeit bearbeitet: 9. September 2020, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryAgentInstallationPolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation des AWS Replication Agent, der zusammen mit AWS Elastic Disaster Recovery (DRS) zur Wiederherstellung externer Server verwendet wird AWS. Ordnen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen zu, deren Anmeldeinformationen Sie bei der Installation des AWS Replication Agent angeben.

`AWSElasticDisasterRecoveryAgentInstallationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryAgentInstallationPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 10:37 UTC
- Bearbeitete Zeit: 27. November 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryAgentPolicy

Beschreibung: Diese Richtlinie ermöglicht die Verwendung des AWS Replication Agents, der zusammen mit AWS Elastic Disaster Recovery (DRS) zur Wiederherstellung von Quellservern verwendet wird AWS. Es wird nicht empfohlen, diese Richtlinie an Ihre IAM-Benutzer oder -Rollen anzuhängen.

`AWSElasticDisasterRecoveryAgentPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryAgentPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 10:32 UTC
- Bearbeitete Zeit: 27. November 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryConsoleFullAccess

Beschreibung: Diese Richtlinie bietet vollen Zugriff auf alle öffentlichen APIs von AWS Elastic Disaster Recovery (DRS) sowie Berechtigungen zum Lesen von KMS-Schlüssel-, License Manager-, Resource Groups, Elastic Load Balancing-, IAM- und EC2-Informationen. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSElasticDisasterRecoveryConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 10:46 UTC
- Bearbeitete Zeit: 16. Oktober 2023, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Beschreibung: Diese Richtlinie bietet vollen Zugriff auf alle öffentlichen APIs von AWS Elastic Disaster Recovery (AWS DRS) sowie auf alle öffentlichen APIs in anderen AWS Services, die von der AWS DRS Console verwendet werden. Fügen Sie diese Richtlinie Ihren Benutzern oder Rollen hinzu.

`AWSElasticDisasterRecoveryConsoleFullAccess_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryConsoleFullAccess_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2023, 13:35 UTC
- Bearbeitete Zeit: 19. Mai 2024, 07:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
```

```
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
```

```
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
```

```
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess32",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess33",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess34",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
```

```
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess35",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ConsoleFullAccess36",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess37",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryConversionServerPolicy

Beschreibung: Diese Richtlinie ist der Instanzrolle des AWS Elastic Disaster Recovery Conversion-Servers zugeordnet. Diese Richtlinie ermöglicht es Elastic Disaster Recovery (DRS) - Konversionsservern, bei denen es sich um EC2-Instances handelt, die von Elastic Disaster Recovery gestartet wurden, mit dem DRS-Service zu kommunizieren. Eine IAM-Rolle mit dieser Richtlinie wird von DRS (als EC2-Instance-Profil) an die DRS-Konvertierungsserver angehängt, die bei Bedarf automatisch von DRS gestartet und beendet werden. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen. DRS-Konvertierungsserver werden von Elastic Disaster Recovery verwendet, wenn Benutzer Quellserver mithilfe der DRS-Konsole, CLI oder API wiederherstellen möchten.

`AWSElasticDisasterRecoveryConversionServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryConversionServerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 13:42 UTC
- Bearbeitete Zeit: 27. November 2023, 13:13 UTC

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

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Beschreibung: Diese Richtlinie ermöglicht es AWS Elastic Disaster Recovery (DRS), kontenübergreifende Replikation und kontenübergreifendes Failback zu unterstützen.

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Mai 2023, 07:16 UTC
- Bearbeitete Zeit: 17. Januar 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryEc2InstancePolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS Replication Agents, der von AWS Elastic Disaster Recovery (DRS) zur Wiederherstellung von Quellservern verwendet wird, die auf EC2 laufen (regionsübergreifend oder azübergreifend). Eine IAM-Rolle mit dieser Richtlinie sollte (als EC2-Instance-Profil) an die EC2-Instances angehängt werden.

`AWSElasticDisasterRecoveryEc2InstancePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryEc2InstancePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Mai 2022, 12:30 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Beschreibung: Sie können die AWSElasticDisasterRecoveryFailbackInstallationPolicy Richtlinie an Ihre IAM-Identitäten anhängen. Diese Richtlinie ermöglicht die Installation des Elastic Disaster Recovery Failback Client, der für ein Failback von Wiederherstellungsinstanzen auf Ihre ursprüngliche Quellinfrastruktur verwendet wird. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu, deren Anmeldeinformationen Sie bei der Ausführung des Elastic Disaster Recovery Failback Client angeben.

`AWSElasticDisasterRecoveryFailbackInstallationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryFailbackInstallationPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 11:02 UTC
- Bearbeitete Zeit: 27. November 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryFailbackPolicy

Beschreibung: Diese Richtlinie ermöglicht die Verwendung des Elastic Disaster Recovery Failback Client, der für ein Failback von Wiederherstellungsinstanzen auf Ihre ursprüngliche Quellinfrastruktur

verwendet wird. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSElasticDisasterRecoveryFailbackPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryFailbackPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 10:41 UTC
- Bearbeitete Zeit: 27. November 2023, 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryLaunchActionsPolicy

Beschreibung: Mit dieser Richtlinie können Sie Amazon SSM und weitere für Dienste erforderliche Berechtigungen verwenden, um Aktionen nach dem Start in AWS Elastic Disaster Recovery (AWS DRS) auszuführen. Hängen Sie diese Richtlinie an Ihre IAM-Rollen oder -Benutzer an.

`AWSElasticDisasterRecoveryLaunchActionsPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryLaunchActionsPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. September 2023, 07:38 UTC
- Bearbeitete Zeit: 19. Mai 2024, 07:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy3",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-*",
        "arn:aws:ssm:*::document/AWSCodeDeployAgent-*",
        "arn:aws:ssm:*::document/AWSConfigRemediation-*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSDisasterRecovery-*",
        "arn:aws:ssm:*::document/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-*:*"
      ],
      "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Beschreibung: Diese Richtlinie ermöglicht es AWS Elastic Disaster Recovery (DRS), die Netzwerkreplikation zu unterstützen.

`AWSElasticDisasterRecoveryNetworkReplicationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryNetworkReplicationPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. Juni 2023, 12:36 UTC
- Bearbeitete Zeit: 2. Januar 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryReadOnlyAccess

Beschreibung: Sie können die AWSElasticDisasterRecoveryReadOnlyAccess Richtlinie an Ihre IAM-Identitäten anhängen. Diese Richtlinie gewährt Berechtigungen für alle schreibgeschützten öffentlichen APIs von Elastic Disaster Recovery (DRS) sowie für einige schreibgeschützte APIs anderer AWS Dienste, die erforderlich sind, um die DRS-Konsole vollständig schreibgeschützt nutzen zu können. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSElasticDisasterRecoveryReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 10:50 UTC
- Bearbeitete Zeit: 27. November 2023, 13:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
```

```
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess4",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess5",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommandInvocations",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess6",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameter",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    },
    {
      "Sid" : "DRSReadOnlyAccess7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-CreateImage",
```

```
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ]
    },
    {
      "Sid" : "DRSReadOnlyAccess8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Beschreibung: Diese Richtlinie ist an die Instanzrolle der Wiederherstellungsinstanz von Elastic Disaster Recovery angehängt. Diese Richtlinie ermöglicht es der Elastic Disaster Recovery (DRS) Recovery Instance, bei der es sich um EC2-Instances handelt, die von Elastic Disaster Recovery gestartet wurden, mit dem DRS-Service zu kommunizieren und auf ihre ursprüngliche

Quellinfrastruktur zurückzugreifen. Eine IAM-Rolle mit dieser Richtlinie wird (als EC2-Instance-Profil) von Elastic Disaster Recovery den DRS-Wiederherstellungsinstanzen zugewiesen. Wir empfehlen nicht, diese Richtlinie an Ihre IAM-Benutzer oder -Rollen anzuhängen.

`AWSElasticDisasterRecoveryRecoveryInstancePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryRecoveryInstancePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 10:20 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryReplicationServerPolicy

Beschreibung: Diese Richtlinie ist der Instance-Rolle des Elastic Disaster Recovery Replication-Servers zugeordnet. Diese Richtlinie ermöglicht es den Elastic Disaster Recovery (DRS) Replication Servern, bei denen es sich um EC2-Instances handelt, die von Elastic Disaster Recovery gestartet wurden, mit dem DRS-Service zu kommunizieren und EBS-Snapshots in Ihrem zu erstellen. AWS-Konto Eine IAM-Rolle mit dieser Richtlinie wird (als EC2-Instance-Profil) von Elastic Disaster Recovery den DRS-Replikationsservern zugewiesen, die bei Bedarf automatisch von DRS gestartet und beendet werden. DRS-Replikationsserver werden verwendet, um die Datenreplikation von Ihren externen Servern auf die AWS Daten als Teil des von DRS verwalteten Wiederherstellungsprozesses zu erleichtern. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSElasticDisasterRecoveryReplicationServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryReplicationServerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 17. November 2021, 13:34 UTC
- Bearbeitete Zeit: 27. November 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht Elastic Disaster Recovery, AWS Ressourcen in Ihrem Namen zu verwalten.

`AWSElasticDisasterRecoveryServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. November 2021, 10:56 UTC
- Bearbeitete Zeit: 17. Januar 2024, 13:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
```

```
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy10",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy16",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy25",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy28",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryStagingAccountPolicy

Beschreibung: Diese Richtlinie ermöglicht den schreibgeschützten Zugriff auf AWS Elastic Disaster Recovery (DRS) -Ressourcen wie Quellserver und Jobs. Sie ermöglicht auch die Erstellung eines konvertierten Snapshots und die gemeinsame Nutzung dieses EBS-Snapshots mit einem bestimmten Konto.

`AWSElasticDisasterRecoveryStagingAccountPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryStagingAccountPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Mai 2022, 09:49 UTC
- Bearbeitete Zeit: 27. November 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Beschreibung: Diese Richtlinie wird von AWS Elastic Disaster Recovery (DRS) verwendet, um Quellserver in einem separaten Zielkonto wiederherzustellen und ein Failback zu ermöglichen. Es wird nicht empfohlen, diese Richtlinie an Ihre IAM-Benutzer oder -Rollen anzuhängen.

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Januar 2023, 12:11 UTC
- Bearbeitete Zeit: 27. November 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticLoadBalancingClassicServiceRolePolicy

Beschreibung: Service Linked Role Policy für AWS Elastic Load Balancing Control Plane — Classic

`AWSElasticLoadBalancingClassicServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. September 2017, 22:36 Uhr UTC
- Bearbeitete Zeit: 7. Oktober 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticLoadBalancingServiceRolePolicy

Beschreibung: Service Linked Role Policy für die AWS Elastic Load Balancing Control Plane

`AWSElasticLoadBalancingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. September 2017, 22:19 Uhr UTC
- Bearbeitete Zeit: 26. August 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
```

```
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:ReleaseAddress",
        "ec2:UnassignIpv6Addresses",
        "ec2:DescribeVpcPeeringConnections",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaConvertFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Elemental MediaConvert über das SDK AWS Management Console und.

`AWSElementalMediaConvertFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaConvertFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juni 2018, 19:25 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaConvertReadOnly

Beschreibung: Bietet MediaConvert über das SDK AWS Management Console und den Lesezugriff auf AWS Elemental.

`AWSElementalMediaConvertReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaConvertReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juni 2018, 19:25 UTC

- Bearbeitete Zeit: 10. Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaLiveFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS elementare Ressourcen MediaLive

`AWSElementalMediaLiveFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaLiveFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Juli 2020, 17:07 UTC
- Bearbeitete Zeit: 8. Juli 2020, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaLiveReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Elementar-Ressourcen MediaLive

`AWSElementalMediaLiveReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaLiveReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Juli 2020, 16:38 UTC
- Bearbeitete Zeit: 8. Juli 2020, 16:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaPackageFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS elementare Ressourcen MediaPackage

`AWSElementalMediaPackageFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaPackageFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. Dezember 2017, 23:39 Uhr UTC

- Zeit bearbeitet: 29. Dezember 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaPackageReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Elementar-Ressourcen MediaPackage

`AWSElementalMediaPackageReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaPackageReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Dezember 2017, 00:04 Uhr UTC
- Zeit bearbeitet: 30. Dezember 2017, 00:04 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaPackageV2FullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Elemental MediaPackage V2-Ressourcen.

`AWSElementalMediaPackageV2FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaPackageV2FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juli 2023, 20:29 UTC
- Bearbeitete Zeit: 25. Juli 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaPackageV2ReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Elemental V2-Ressourcen MediaPackage.

`AWSElementalMediaPackageV2ReadOnly`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaPackageV2ReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juli 2023, 20:31 UTC
- Bearbeitete Zeit: 25. Juli 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaStoreFullAccess

Beschreibung: Bietet vollständigen Lese- und Schreibzugriff auf alle MediaStore APIs

`AWSElementalMediaStoreFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaStoreFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 5. März 2018, 23:15 Uhr UTC
- Bearbeitete Zeit: 5. März 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaStoreReadOnly

Beschreibung: Stellt Nur-Lese-Berechtigungen für APIs bereit MediaStore

`AWSElementalMediaStoreReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaStoreReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. März 2018, 19:48 UTC
- Bearbeitete Zeit: 8. März 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaTailorFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS elementare Ressourcen MediaTailor

`AWSElementalMediaTailorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaTailorFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. November 2021, 00:04 Uhr UTC
- Bearbeitete Zeit: 23. November 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaTailorReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Elementar-Ressourcen MediaTailor

`AWSElementalMediaTailorReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSElementalMediaTailorReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. November 2021, 00:05 Uhr UTC
- Bearbeitete Zeit: 23. November 2021, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEnhancedClassicNetworkingMangementPolicy

Beschreibung: Richtlinie zur Aktivierung der erweiterten klassischen Netzwerkverwaltungsfunktion.

`AWSEnhancedClassicNetworkingMangementPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. September 2017, 17:29 Uhr UTC
- Zeit bearbeitet: 20. September 2017, 17:29 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
```

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEntityResolutionConsoleFullAccess

Beschreibung: Bietet vollen Konsolenzugriff auf AWS Entity Resolution und verwandte Dienste.

`AWSEntityResolutionConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSEntityResolutionConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. August 2023, 17:54 UTC
- Bearbeitete Zeit: 16. Oktober 2023, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEntityResolutionConsoleReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Entity Resolution über die. AWS Management Console

`AWSEntityResolutionConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSEntityResolutionConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. August 2023, 18:18 UTC
- Bearbeitete Zeit: 17. August 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionRead",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:Get*",
        "entityresolution:List*"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorEC2Access

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service in EC2 und anderen erforderlichen Diensten die Erlaubnis, FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorEC2Access`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFaultInjectionSimulatorEC2Access` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:39 UTC
- Bearbeitete Zeit: 27. November 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorECSAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service in ECS und anderen erforderlichen Diensten die Erlaubnis, FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorECSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFaultInjectionSimulatorECSAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:37 UTC
- Bearbeitete Zeit: 25. Januar 2024, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorEKSAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service in EKS und anderen erforderlichen Diensten die Berechtigung, FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorEKSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFaultInjectionSimulatorEKSAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:34 UTC
- Bearbeitete Zeit: 13. November 2023, 16:44 UTC

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

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorNetworkAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service die Erlaubnis, in EC2-Netzwerken und anderen erforderlichen Diensten FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorNetworkAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFaultInjectionSimulatorNetworkAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 26. Oktober 2022, 20:32 UTC
- Bearbeitete Zeit: 25. Januar 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorRDSAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service in RDS und anderen erforderlichen Diensten die Erlaubnis, FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorRDSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFaultInjectionSimulatorRDSAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:30 Uhr UTC
- Bearbeitete Zeit: 13. November 2023, 16:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorSSMAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service in SSM und anderen erforderlichen Diensten die Berechtigung, FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorSSMAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFaultInjectionSimulatorSSMAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 15:33 UTC
- Bearbeitete Zeit: 2. Juni 2023, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFinSpaceServiceRolePolicy

Beschreibung: Richtlinie zur Aktivierung des Zugriffs auf AWS-Service und von Amazon verwendete oder verwaltete Ressourcen FinSpace

`AWSFinSpaceServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Mai 2023, 16:42 UTC
- Bearbeitete Zeit: 1. Dezember 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFMAdminFullAccess

Beschreibung: Voller Zugriff für AWS FM Administrator

`AWSFMAdminFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFMAdminFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Mai 2018, 18:06 UTC
- Zeit bearbeitet: 20. Oktober 2022, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFMAdminReadOnlyAccess

Beschreibung: Nur-Lese-Zugriff für AWS FM Administrator, der die Überwachung von AWS FM-Vorgängen ermöglicht

`AWSFMAdminReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFMAdminReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Mai 2018, 20:07 UTC
- Bearbeitete Zeit: 31. Oktober 2022, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

```
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFMMemberReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS WAF-Aktionen für AWS Firewall Manager Manager-Mitgliedskonten

`AWSFMMemberReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSFMMemberReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Mai 2018, 21:05 UTC
- Bearbeitete Zeit: 9. Mai 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSForWordPressPluginPolicy

Beschreibung: Verwaltete Richtlinie für das AWS For Wordpress Plugin

`AWSForWordPressPluginPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSForWordPressPluginPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Oktober 2019, 00:27 UTC
- Bearbeitete Zeit: 20. Januar 2020, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGitSyncServiceRolePolicy

Beschreibung: Richtlinie, die es AWS Code Connections ermöglicht, Inhalte aus Ihrem Git-Repository zu synchronisieren

`AWSGitSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. November 2023, 17:05 UTC

- Bearbeitete Zeit: 26. April 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlobalAcceleratorSLRPolicy

Beschreibung: Richtlinie, die AWS Global Accelerator Berechtigungen zur Verwaltung von EC2 Elastic Network Interfaces und Security Groups gewährt.

`AWSGlobalAcceleratorSLRPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. April 2019, 19:39 UTC
- Bearbeitete Zeit: 12. September 2023, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Glue über AWS Management Console

`AWSGlueConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGlueConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. August 2017, 13:37 UTC
- Bearbeitete Zeit: 14. Juli 2023, 14:37 UTC

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

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueConsoleSageMakerNotebookFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Glue über die AWS Management Console und Zugriff auf Sagemaker-Notebook-Instanzen.

`AWSGlueConsoleSageMakerNotebookFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGlueConsoleSageMakerNotebookFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 5. Oktober 2018, 17:52 Uhr UTC
- Bearbeitete Zeit: 15. Juli 2021, 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueDataBrewFullAccessPolicy

Beschreibung: Bietet vollen Zugriff auf AWS Glue DataBrew über die AWS Management Console. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, KMS, Glue).

`AwsGlueDataBrewFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AwsGlueDataBrewFullAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. November 2020, 16:51 UTC
- Zeit bearbeitet: 4. Februar 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueDataBrewServiceRole

Beschreibung: Diese Richtlinie gewährt Glue die Erlaubnis, Aktionen für den Glue-Datenkatalog des Benutzers auszuführen. Diese Richtlinie gewährt auch die Erlaubnis für ec2-Aktionen, damit Glue ENI erstellen kann, um eine Verbindung zu Ressourcen in der VPC herzustellen, Glue auch den Zugriff auf registrierte Daten in Lakeformation und die Erlaubnis, auf die Cloudwatch des Benutzers zuzugreifen

`AWSGlueDataBrewServiceRole`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGlueDataBrewServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. Dezember 2020, 21:26 Uhr UTC
- Bearbeitete Zeit: 20. März 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueSchemaRegistryFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Glue Schema Registry Service

`AWSGlueSchemaRegistryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGlueSchemaRegistryFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2020, 00:19 UTC
- Zeit bearbeitet: 20. November 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueSchemaRegistryReadonlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den AWS Glue Schema Registry Service

`AWSGlueSchemaRegistryReadonlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGlueSchemaRegistryReadonlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 20. November 2020, 00:20 UTC
- Zeit bearbeitet: 20. November 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueServiceNotebookRole

Beschreibung: Richtlinie für die AWS Glue-Servicerolle, die es dem Kunden ermöglicht, den Notebook-Server zu verwalten

`AWSGlueServiceNotebookRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGlueServiceNotebookRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:37 Uhr UTC
- Bearbeitete Zeit: 9. Oktober 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueServiceRole

Beschreibung: Richtlinie für die AWS Glue-Dienstrolle, die den Zugriff auf verwandte Dienste wie EC2, S3 und Cloudwatch Logs ermöglicht

`AWSGlueServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGlueServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:37 UTC
- Bearbeitete Zeit: 11. September 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedNotebookPolicy

Beschreibung: Stellt Berechtigungen bereit, die es Benutzern ermöglichen, nur die Notizbuchsitzungen zu erstellen und zu verwenden, die dem Benutzer zugeordnet sind. Diese Richtlinie beinhaltet auch Berechtigungen, die es Benutzern ausdrücklich ermöglichen, eine eingeschränkte Glue-Sitzungsrolle zu übergeben.

`AwsGlueSessionUserRestrictedNotebookPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AwsGlueSessionUserRestrictedNotebookPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. April 2022, 15:24 UTC
- Zeit bearbeitet: 22. November 2023, 01:32 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "NotebookAllowActions1",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "NotebookAllowActions2",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions3",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "NotebookDenyActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "NotebookPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AwsGlueSessionServiceRoleUserRestrictedForNotebook*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedNotebookServiceRole

Beschreibung: Bietet vollen Zugriff auf alle AWS Glue-Ressourcen mit Ausnahme von Sitzungen. Ermöglicht Benutzern, nur die Notebook-Sitzungen zu erstellen und zu verwenden, die mit dem Benutzer verknüpft sind. Diese Richtlinie umfasst auch andere Berechtigungen, die Glue benötigt, um AWS Glue-Ressourcen in anderen AWS Diensten zu verwalten.

`AwsGlueSessionUserRestrictedNotebookServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AwsGlueSessionUserRestrictedNotebookServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 18. April 2022, 15:27 UTC
- Bearbeitete Zeit: 18. April 2022, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedPolicy

Beschreibung: Stellt Berechtigungen bereit, die es Benutzern ermöglichen, nur die interaktiven Sitzungen zu erstellen und zu verwenden, die dem Benutzer zugeordnet sind. Diese Richtlinie beinhaltet auch Berechtigungen, die es Benutzern ausdrücklich ermöglichen, eine eingeschränkte Glue-Sitzungsrolle zu übergeben.

`AwsGlueSessionUserRestrictedPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AwsGlueSessionUserRestrictedPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. April 2022, 21:31 UTC
- Bearbeitete Zeit: 29. April 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedServiceRole

Beschreibung: Bietet vollen Zugriff auf alle AWS Glue-Ressourcen mit Ausnahme von Sitzungen. Ermöglicht Benutzern, nur die interaktiven Sitzungen zu erstellen und zu verwenden, die mit dem Benutzer verknüpft sind. Diese Richtlinie umfasst auch andere Berechtigungen, die Glue benötigt, um AWS Glue-Ressourcen in anderen AWS Diensten zu verwalten.

`AwsGlueSessionUserRestrictedServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AwsGlueSessionUserRestrictedServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. April 2022, 21:30 UTC
- Bearbeitete Zeit: 29. April 2024, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStatementActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessionsAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
```

```
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectCrawlerActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Sid" : "AllowLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Sid" : "AllowTagsActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGrafanaAccountAdministrator

Beschreibung: Ermöglicht den Zugriff innerhalb von Amazon Grafana zum Erstellen und Verwalten von Arbeitsbereichen für das gesamte Unternehmen.

`AWSGrafanaAccountAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGrafanaAccountAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Februar 2021, 00:20 UTC
- Bearbeitete Zeit: 15. Februar 2022, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGrafanaConsoleReadOnlyAccess

Beschreibung: Zugriff auf schreibgeschützte Operationen in Amazon Grafana.

`AWSGrafanaConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGrafanaConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Februar 2021, 00:10 UTC
- Bearbeitete Zeit: 15. Februar 2022, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGrafanaWorkspacePermissionManagement

Beschreibung: Bietet nur die Möglichkeit, Benutzer- und Gruppenberechtigungen für AWS Grafana-Arbeitsbereiche zu aktualisieren.

`AWSGrafanaWorkspacePermissionManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGrafanaWorkspacePermissionManagement` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Februar 2021, 00:15 UTC
- Bearbeitete Zeit: 15. März 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGrafanaWorkspacePermissionManagementV2

Beschreibung: Bietet die Möglichkeit, Benutzer- und Gruppenberechtigungen für IAM Identity Center (IdC) für Amazon Managed Grafana-Arbeitsbereiche zu aktualisieren.

`AWSGrafanaWorkspacePermissionManagementV2`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGrafanaWorkspacePermissionManagementV2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Januar 2024, 18:39 UTC

- Bearbeitungszeit: 5. Januar 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGreengrassFullAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf die Konfiguration, Verwaltung und Bereitstellung von AWS Greengrass

`AWSGreengrassFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGreengrassFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Mai 2017, 00:47 UTC
- Zeit bearbeitet: 3. Mai 2017, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGreengrassReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Lesezugriff auf die AWS Greengrass-Konfiguration, Verwaltung und Bereitstellung.

`AWSGreengrassReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGreengrassReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Oktober 2018, 16:01 UTC
- Bearbeitete Zeit: 30. Oktober 2018, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGreengrassResourceAccessRolePolicy

Beschreibung: Richtlinie für die AWS Greengrass-Dienstrolle, die den Zugriff auf verwandte Dienste wie AWS Lambda und AWS IoT-Ding-Shadows ermöglicht.

`AWSGreengrassResourceAccessRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGreengrassResourceAccessRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Februar 2017, 21:17 UTC
- Zeit bearbeitet: 14. November 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGroundStationAgentInstancePolicy

Beschreibung: Stellt der Dataflow Endpoint Instance Berechtigungen zur Verwendung des AWS Ground Station Agents zur Verfügung

`AWSGroundStationAgentInstancePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSGroundStationAgentInstancePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. März 2023, 15:23 UTC
- Bearbeitete Zeit: 29. März 2023, 15:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSHealth_EventProcessorServiceRolePolicy

Beschreibung: Ermöglicht AWS Health, die Health Event Processor-Funktion zu aktivieren.

`AWSHealth_EventProcessorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Januar 2023, 19:24 UTC
- Bearbeitete Zeit: 13. Januar 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSHealthFullAccess

Beschreibung: Ermöglicht den vollen Zugriff auf die AWS Health Apis und Benachrichtigungen sowie das Personal Health Dashboard

`AWSHealthFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSHealthFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2016, 12:30 Uhr UTC
- Zeit bearbeitet: 16. November 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSHealthImagingFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Health Imaging-Service.

`AWSHealthImagingFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSHealthImagingFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juli 2023, 23:39 UTC
- Bearbeitete Zeit: 25. Juli 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSHealthImagingReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den AWS Health Imaging-Dienst.

`AWSHealthImagingReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSHealthImagingReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juli 2023, 23:40 UTC
- Bearbeitete Zeit: 1. August 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIAMIdentityCenterAllowListForIdentityContext

Beschreibung: Stellt die Liste der Aktionen bereit, die für Rollen zulässig sind, die im IAM Identity Center-Identitätskontext übernommen wurden. AWS Der Security Token Service (AWS STS) ordnet diese Richtlinie automatisch den übernommenen Rollen zu. Der Identitätskontext wird als ProvidedContext übergeben.

`AWSIAMIdentityCenterAllowListForIdentityContext`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIAMIdentityCenterAllowListForIdentityContext` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 08. November 2023, 15:21 UTC
- Bearbeitete Zeit: 16. Mai 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
```

```
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:ListSteps",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
```

```
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "qapps:CreateQApp",
        "qapps:PredictProblemStatementFromConversation",
        "qapps:PredictQAppFromProblemStatement",
        "qapps:CopyQApp",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:UpdateQApp",
        "qapps:DeleteQApp",
        "qapps:AssociateQAppWithUser",
        "qapps:DisassociateQAppFromUser",
        "qapps:ImportDocumentToQApp",
        "qapps:ImportDocumentToQAppSession",
        "qapps:CreateLibraryItem",
        "qapps:GetLibraryItem",
        "qapps:UpdateLibraryItem",
        "qapps:CreateLibraryItemReview",
        "qapps:ListLibraryItems",
        "qapps:CreateSubscriptionToken",
        "qapps:StartQAppSession",
        "qapps:StopQAppSession",
        "qbusiness:Chat",
        "qbusiness:ChatSync",
        "qbusiness:ListConversations",
        "qbusiness:ListMessages",
        "qbusiness:DeleteConversation",
        "qbusiness:PutFeedback",
        "sts:SetContext"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIdentitySyncFullAccess

Beschreibung: Gewährt vollen Zugriff auf den Identity Sync-Dienst

`AWSIdentitySyncFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIdentitySyncFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. März 2022, 23:29 UTC
- Bearbeitete Zeit: 23. März 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIdentitySyncReadOnlyAccess

Beschreibung: Schreibgeschützter Zugriff auf den Identity Sync-Dienst

`AWSIdentitySyncReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIdentitySyncReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. März 2022, 23:29 UTC
- Bearbeitete Zeit: 23. März 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSImageBuilderFullAccess

Beschreibung: Bietet vollen Zugriff auf alle AWS Image Builder Builder-Aktionen und ressourcenspezifischen Zugriff auf zugehörige AWS Dienste.

`AWSImageBuilderFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSImageBuilderFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. Dezember 2019, 18:25 Uhr UTC
- Bearbeitete Zeit: 13. April 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSImageBuilderReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle AWS Image Builder Builder-Aktionen.

`AWSImageBuilderReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSImageBuilderReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Dezember 2019, 22:29 Uhr UTC
- Bearbeitete Zeit: 19. Dezember 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSImportExportFullAccess

Beschreibung: Bietet Lese- und Schreibzugriff auf die Jobs, die unter dem erstellt wurden AWS-Konto.

`AWSImportExportFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSImportExportFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSImportExportReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die Jobs, die unter dem erstellt wurden AWS-Konto.

`AWSImportExportReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSImportExportReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIncidentManagerIncidentAccessServiceRolePolicy

Beschreibung: Erteilt Incident Manager die Berechtigung, im Rahmen der Verwaltung eines Vorfalls andere AWS Dienste aufzurufen.

`AWSIncidentManagerIncidentAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIncidentManagerIncidentAccessServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2023, 00:01 UTC
- Bearbeitete Zeit: 20. Februar 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIncidentManagerResolverAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen zum Starten, Anzeigen und Aktualisieren von Vorfällen mit vollem Zugriff auf benutzerdefinierte Ereignisse und verwandte Elemente in der Zeitleiste. Weisen Sie diese Richtlinie Benutzern zu, die Vorfälle erstellen und lösen.

`AWSIncidentManagerResolverAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIncidentManagerResolverAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 10. Mai 2021, 06:12 UTC
- Bearbeitete Zeit: 10. Mai 2021, 06:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:GetIncidentRecord",
```

```
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:DeleteTimelineEvent",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:UpdateRelatedItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIncidentManagerServiceRolePolicy

Beschreibung: Diese Richtlinie gewährt Incident Manager die Erlaubnis, Incident-Aufzeichnungen und zugehörige Ressourcen in Ihrem Namen zu verwalten.

`AWSIncidentManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Mai 2021, 03:34 UTC

- Bearbeitete Zeit: 5. Dezember 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoT1ClickFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS IoT 1-Click.

`AWSIoT1ClickFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoT1ClickFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2018, 22:10 Uhr UTC
- Bearbeitete Zeit: 11. Mai 2018, 22:10 UTC

- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoT1ClickReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS IoT 1-Click.

`AWSIoT1ClickReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoT1ClickReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2018, 21:49 UTC
- Bearbeitete Zeit: 11. Mai 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTAnalyticsFullAccess

Beschreibung: Bietet vollen Zugriff auf IoT Analytics.

`AWSIoTAnalyticsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTAnalyticsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juni 2018, 23:02 UTC
- Bearbeitete Zeit: 18. Juni 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTAnalyticsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IoT Analytics.

`AWSIoTAnalyticsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTAnalyticsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juni 2018, 21:37 UTC

- Bearbeitete Zeit: 18. Juni 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTConfigAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf die AWS IoT-Konfigurationsaktionen

`AWSIoTConfigAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTConfigAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Oktober 2015, 21:52 Uhr UTC
- Bearbeitete Zeit: 27. September 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTConfigReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Lesezugriff auf die AWS IoT-Konfigurationsaktionen

`AWSIoTConfigReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTConfigReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Oktober 2015, 21:52 UTC
- Bearbeitete Zeit: 27. September 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDataAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf die AWS IoT-Messaging-Aktionen

`AWSIoTDataAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDataAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Oktober 2015, 21:51 UTC
- Bearbeitete Zeit: 23. Juni 2021, 21:34 UTC

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

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Beschreibung: Bietet Schreibzugriff auf IoT-Dinggruppen und Lesezugriff auf IoT-Zertifikate für die Ausführung von ADD_THINGS_TO_THING_GROUP Risikominderungsmaßnahmen

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:55 Uhr UTC
- Bearbeitete Zeit: 7. August 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Effect" : "Allow",
      "Action" : [
        "iot:ListPrincipalThings",
        "iot:AddThingToThingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderAudit

Beschreibung: Bietet Lesezugriff für IoT und verwandte Ressourcen

`AWSIoTDeviceDefenderAudit`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDeviceDefenderAudit` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 18. Juli 2018, 21:17 Uhr UTC
- Bearbeitete Zeit: 25. November 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Beschreibung: Ermöglicht den Zugriff auf die Aktivierung der IoT-Protokollierung für die Ausführung der ENABLE_IOT_LOGGING-Minderungsaktion

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:04 UTC
- Bearbeitete Zeit: 7. August 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Beschreibung: Ermöglicht die Veröffentlichung von Nachrichten auf das SNS-Thema zur Ausführung der Public_FINDING_TO_SNS-Abhilfemaßnahmen

`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:04 UTC
- Bearbeitete Zeit: 7. August 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Beschreibung: Bietet Schreibzugriff auf IoT-Richtlinien für die Ausführung von REPLACE_DEFAULT_POLICY_VERSION-Minderungsmaßnahmen

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 7. August 2019, 17:04 UTC
- Bearbeitete Zeit: 7. August 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Beschreibung: Bietet Schreibzugriff auf IoT-CA-Zertifikate für die Ausführung von UPDATE_CA_CERTIFICATE-Abhilfemaßnahmen

`AWSIoTDeviceDefenderUpdateCACertMitigationAction`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDeviceDefenderUpdateCACertMitigationAction` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:05 UTC
- Bearbeitete Zeit: 7. August 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "iot:UpdateCACertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Beschreibung: Bietet Schreibzugriff auf IoT-Zertifikate für die Ausführung von UPDATE_DEVICE_CERTIFICATE-Abhilfemaßnahmen

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:06 UTC
- Bearbeitete Zeit: 7. August 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceTesterForFreeRTOSFullAccess

Beschreibung: Ermöglicht AWS IoT Device Tester, die FreeRTOS-Qualifizierungssuite auszuführen, indem der Zugriff auf Dienste wie IoT, S3 und IAM ermöglicht wird

`AWSIoTDeviceTesterForFreeRTOSFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDeviceTesterForFreeRTOSFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Februar 2020, 20:33 UTC
- Bearbeitete Zeit: 10. August 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceTesterForGreengrassFullAccess

Beschreibung: Ermöglicht AWS IoT Device Tester, die AWS Greengrass-Qualifizierungssuite auszuführen, indem der Zugriff auf verwandte Dienste wie Lambda, IoT, API Gateway und IAM ermöglicht wird

`AWSIoTDeviceTesterForGreengrassFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTDeviceTesterForGreengrassFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. Februar 2020, 21:21 UTC
- Bearbeitete Zeit: 25. Juni 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTEventsFullAccess

Beschreibung: Bietet vollen Zugriff auf IoT Events.

`AWSIoTEventsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTEventsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. Januar 2019, 22:51 UTC
- Bearbeitete Zeit: 10. Januar 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTEventsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IoT Events.

`AWSIoTEventsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTEventsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. Januar 2019, 22:50 UTC
- Bearbeitete Zeit: 23. September 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:Describe*",
        "iotevents:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTFleetHubFederationAccess

Beschreibung: Verbundzugriff für IoT Fleet Hub-Anwendungen

`AWSIoTFleetHubFederationAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTFleetHubFederationAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 15. Dezember 2020, 08:08 UTC
- Bearbeitete Zeit: 4. April 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTFleetwiseServiceRolePolicy

Beschreibung: Gewährt Berechtigungen für AWS Ressourcen und Metadaten, die AWSIoTFleetwise für zusätzliche Funktionen verwendet oder verwaltet werden

`AWSIoTFleetwiseServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. September 2022, 23:27 UTC
- Bearbeitete Zeit: 21. September 2022, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTFullAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf die AWS IoT-Konfiguration und die Messaging-Aktionen

`AWSIoTFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Oktober 2015, 15:19 Uhr UTC
- Bearbeitete Zeit: 19. Mai 2022, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTLogging

Beschreibung: Ermöglicht die Erstellung von Amazon CloudWatch Log-Gruppen und das Streamen von Protokollen an die Gruppen

`AWSIoTLogging`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTLogging` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Oktober 2015, 15:17 Uhr UTC
- Zeit bearbeitet: 8. Oktober 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs:DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTOTAUpdate

Beschreibung: Ermöglicht den Zugriff auf die Erstellung eines AWS IoT-Jobs und die Beschreibung des AWS Codesigner-Jobs

`AWSIoTOTAUpdate`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTOTAUpdate` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. Dezember 2017, 20:36 Uhr UTC
- Bearbeitete Zeit: 20. Dezember 2017, 20:36 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIotRoboRunnerFullAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die den vollen Zugriff auf AWS IoT ermöglichen RoboRunner.

`AWSIotRoboRunnerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIotRoboRunnerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 03:54 UTC
- Bearbeitete Zeit: 23. Februar 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIotRoboRunnerReadOnly

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die einen schreibgeschützten Zugriff auf IoT ermöglichen. AWS RoboRunner

`AWSIotRoboRunnerReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIotRoboRunnerReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 03:43 UTC
- Zeit bearbeitet: 16. November 2022, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIotRoboRunnerServiceRolePolicy

Beschreibung: Ermöglicht AWS IoT RoboRunner , zugehörige AWS Ressourcen im Namen des Kunden zu verwalten.

`AWSIotRoboRunnerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Februar 2023, 16:56 UTC
- Bearbeitete Zeit: 21. Februar 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        ]
      }
    }
  }
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTRuleActions

Beschreibung: Ermöglicht den Zugriff auf alle AWS Dienste, die in AWS IoT-Regelaktionen unterstützt werden

`AWSIoTRuleActions`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTRuleActions` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Oktober 2015, 15:14 Uhr UTC
- Bearbeitete Zeit: 16. Januar 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung SiteWise von AWS IoT mithilfe der AWS Management Console. Beachten Sie, dass diese Richtlinie auch Zugriff auf das Erstellen und Auflisten von mit AWS IoT verwendeten Datenspeichern SiteWise (z. B. AWS IoT Analytics), Zugriff auf das Auflisten und Anzeigen von AWS IoT Greengrass-Ressourcen, das Auflisten und Ändern

von AWS Secrets Manager Manager-Geheimnissen, das Abrufen von AWS IoT-Dingschatten, das Auflisten von Ressourcen mit bestimmten Tags und das Erstellen und Verwenden einer dienstbezogenen Rolle für AWS IoT gewährt. SiteWise

`AWSIoTSiteWiseConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTSiteWiseConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Mai 2019, 21:37 UTC
- Bearbeitete Zeit: 31. Mai 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseFullAccess

Beschreibung: Bietet vollen Zugriff auf IoT SiteWise.

`AWSIoTSiteWiseFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTSiteWiseFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Dezember 2018, 20:53 UTC
- Bearbeitete Zeit: 4. Dezember 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseMonitorPortalAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen für den Zugriff auf AWS SiteWise IoT-Assets und Asset-Daten, die Erstellung von AWS SiteWise IoT-Monitor-Ressourcen und die Auflistung von AWS SSO-Benutzern.

`AWSIoTSiteWiseMonitorPortalAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTSiteWiseMonitorPortalAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. Mai 2020, 20:01 Uhr UTC
- Bearbeitete Zeit: 19. Mai 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseMonitorServiceRolePolicy

Beschreibung: Diese Rolle gewährt AWS SiteWise IoT-Monitorberechtigungen für den Zugriff auf Ihre AWS SiteWise IoT-Assets und Asset-Eigenschaften sowie für die Erstellung AWS von Sitewise-Projekten, -Dashboards und Zugriffsrichtlinien für AWS IoT über SiteWise IoT-Portale.

`AWSIoTSiteWiseMonitorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2019, 00:59 UTC
- Bearbeitete Zeit: 13. Dezember 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IoT SiteWise.

`AWSIoTSiteWiseReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTSiteWiseReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Dezember 2018, 20:55 UTC
- Bearbeitete Zeit: 16. September 2022, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTThingsRegistration

Beschreibung: Diese Richtlinie ermöglicht es Benutzern, Dinge mithilfe der AWS StartThingRegistrationTask IoT-API massenweise zu registrieren

`AWSIoTThingsRegistration`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTThingsRegistration` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 1. Dezember 2017, 20:21 Uhr UTC
- Zeit bearbeitet: 5. Oktober 2020, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTTwinMakerServiceRolePolicy

Beschreibung: Ermöglicht AWS IoT TwinMaker , andere AWS Dienste anzurufen und deren Ressourcen in Ihrem Namen zu synchronisieren.

`AWSIoTTwinMakerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. November 2023, 18:59 UTC
- Bearbeitete Zeit: 13. November 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessDataAccess

Beschreibung: Ermöglicht den zugehörigen Identitätsdatenzugriff auf AWS IoT-Wireless-Geräte.

`AWSIoTWirelessDataAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTWirelessDataAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:31 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessFullAccess

Beschreibung: Ermöglicht der zugehörigen Identität den vollen Zugriff auf alle AWS IoT-Wireless-Operationen.

`AWSIoTWirelessFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTWirelessFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:27 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:27 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessFullPublishAccess

Beschreibung: Bietet vollen Zugriff auf IoT Wireless, sodass Sie in Ihrem Namen auf der IoT Rules Engine veröffentlichen können.

`AWSIoTWirelessFullPublishAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTWirelessFullPublishAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:29 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessGatewayCertManager

Beschreibung: Ermöglicht dem zugehörigen Identitätszugriff das Erstellen, Auflisten und Beschreiben von IoT-Zertifikaten

`AWSIoTWirelessGatewayCertManager`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTWirelessGatewayCertManager` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:30 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:30 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessLogging

Beschreibung: Ermöglicht der zugehörigen Identität, Amazon CloudWatch Logs-Gruppen zu erstellen und Protokolle an die Gruppen zu streamen.

`AWSIoTWirelessLogging`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTWirelessLogging` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:32 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessReadOnlyAccess

Beschreibung: Ermöglicht der zugehörigen Identität nur Lesezugriff auf AWS IoT-WLAN.

`AWSIoTWirelessReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIoTWirelessReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:28 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIPAMServiceRolePolicy

Beschreibung: Ermöglicht VPC IP Address Manager den Zugriff auf VPC-Ressourcen und die Integration mit AWS Organizations in Ihrem Namen.

`AWSIPAMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2021, 19:08 UTC

- Bearbeitete Zeit: 8. November 2023, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIQContractServiceRolePolicy

Beschreibung: Wird von AWS IQ verwendet, um Zahlungsanforderungen im Namen eines Kunden auszuführen

`AWSIQContractServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 22. August 2019, 19:28 UTC
- Bearbeitete Zeit: 22. August 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIQFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS IQ

`AWSIQFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSIQFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. April 2019, 23:13 UTC
- Bearbeitete Zeit: 25. September 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIQPermissionServiceRolePolicy

Beschreibung: Ermöglicht AWS IQ, die von AWS IQ-Experten übernommene Rolle zu verwalten.

`AWSIQPermissionServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. August 2019, 19:36 UTC
- Bearbeitete Zeit: 22. August 2019, 19:36 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Dienste und Ressourcen, die für benutzerdefinierte AWS KMS-Schlüsselspeicher erforderlich sind

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2018, 20:10 UTC
- Bearbeitete Zeit: 10. November 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Beschreibung: Ermöglicht AWS KMS, die gemeinsamen Eigenschaften von Schlüsseln mit mehreren Regionen zu synchronisieren.

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Juni 2021, 15:37 UTC
- Bearbeitete Zeit: 16. Juni 2021, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSKeyManagementServicePowerUser

Beschreibung: Ermöglicht den Zugriff auf den AWS Key Management Service (KMS).

`AWSKeyManagementServicePowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSKeyManagementServicePowerUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 7. März 2017, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLakeFormationCrossAccountManager

Beschreibung: Ermöglicht kontenübergreifenden Zugriff auf Glue-Ressourcen über Lake Formation. Gewährt außerdem Lesezugriff auf andere erforderliche Dienste wie Organisationen und den Resource Access Manager

`AWSLakeFormationCrossAccountManager`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLakeFormationCrossAccountManager` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. August 2020, 20:59 UTC
- Bearbeitete Zeit: 22. März 2024, 18:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AllowManageResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowXAcctManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
```

```
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLakeFormationDataAdmin

Beschreibung: Gewährt administrativen Zugriff auf AWS Lake Formation und verwandte Dienste wie AWS Glue zur Verwaltung von Data Lakes

`AWSLakeFormationDataAdmin`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLakeFormationDataAdmin` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. August 2019, 17:33 Uhr UTC
- Bearbeitete Zeit: 22. März 2024, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
```

```
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSLakeFormationDataAdminDeny",
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambda_FullAccess

Beschreibung: Gewährt vollen Zugriff auf den AWS Lambda-Dienst, die Funktionen der AWS Lambda-Konsole und andere zugehörige AWS Dienste.

`AWSLambda_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambda_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2020, 21:14 UTC
- Bearbeitete Zeit: 17. November 2020, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambda_ReadOnlyAccess

Beschreibung: Gewährt schreibgeschützten Zugriff auf den AWS Lambda-Dienst, die Funktionen der AWS Lambda-Konsole und andere verwandte Dienste. AWS

`AWSLambda_ReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambda_ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2020, 21:10 Uhr UTC
- Bearbeitete Zeit: 27. Juli 2023, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "lambda:Get*",
        "lambda:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
```

```
        "logs:DescribeQueries",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaBasicExecutionRole

Beschreibung: Stellt Schreibberechtigungen für CloudWatch Protokolle bereit.

`AWSLambdaBasicExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaBasicExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. April 2015, 15:03 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaDynamoDBExecutionRole

Beschreibung: Bietet Listen- und Lesezugriff auf DynamoDB-Streams sowie Schreibberechtigungen für Protokolle. CloudWatch

`AWSLambdaDynamoDBExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaDynamoDBExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. April 2015, 15:09 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaENIManagementAccess

Beschreibung: Stellt Mindestberechtigungen für eine Lambda-Funktion zur Verwaltung von ENIs (Erstellen, Beschreiben, Löschen) bereit, die von einer VPC-fähigen Lambda-Funktion verwendet werden.

`AWSLambdaENIManagementAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaENIManagementAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Dezember 2016, 00:37 UTC
- Bearbeitete Zeit: 1. Oktober 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaExecute

Beschreibung: Bietet Put, Get Zugriff auf S3 und vollen Zugriff auf CloudWatch Logs.

`AWSLambdaExecute`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaExecute` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaFullAccess

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https:// docs.aws.amazon.com/lambda/latest/dg/ access-control-identity-based .html. Bietet vollen Zugriff auf Lambda, S3, DynamoDB, CloudWatch Metriken und Protokolle.

`AWSLambdaFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 27. November 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaInvocation-DynamoDB

Beschreibung: Bietet Lesezugriff auf DynamoDB Streams.

`AWSLambdaInvocation-DynamoDB`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaInvocation-DynamoDB` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaKinesisExecutionRole

Beschreibung: Bietet Listen- und Lesezugriff auf Kinesis-Streams sowie Schreibberechtigungen für CloudWatch Protokolle.

`AWSLambdaKinesisExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaKinesisExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. April 2015, 15:14 Uhr UTC
- Bearbeitete Zeit: 19. November 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaMSKExecutionRole

Beschreibung: Stellt die erforderlichen Berechtigungen bereit, um auf den MSK-Cluster innerhalb einer VPC zuzugreifen, ENIs (Erstellen, Beschreiben, Löschen) in der VPC zu verwalten und Berechtigungen für Protokolle zu schreiben. CloudWatch

`AWSLambdaMSKExecutionRole`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaMSKExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. August 2020, 17:35 Uhr UTC
- Bearbeitete Zeit: 2. August 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaReplicator

Beschreibung: Gewährt Lambda Replicator die erforderlichen Berechtigungen, um Funktionen regionsübergreifend zu replizieren

`AWSLambdaReplicator`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 23. Mai 2017, 17:53 Uhr UTC
- Zeit bearbeitet: 8. Dezember 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaRole

Beschreibung: Standardrichtlinie für die AWS Lambda-Servicerolle.

`AWSLambdaRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaSQSQueueExecutionRole

Beschreibung: Bietet Zugriff auf SQS-Warteschlangen zum Empfangen von Nachrichten, Löschen von Nachrichten und Lesen von Attributen sowie Schreibberechtigungen für Protokolle. CloudWatch

`AWSLambdaSQSQueueExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaSQSQueueExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Juni 2018, 21:50 Uhr UTC
- Bearbeitete Zeit: 14. Juni 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaVPCAccessExecutionRole

Beschreibung: Stellt Mindestberechtigungen für die Ausführung einer Lambda-Funktion beim Zugriff auf eine Ressource in einer VPC bereit — Netzwerkschnittstellen erstellen, beschreiben, löschen und Schreibberechtigungen für Logs. CloudWatch

`AWSLambdaVPCAccessExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLambdaVPCAccessExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. Februar 2016, 23:15 Uhr UTC
- Bearbeitete Zeit: 5. Januar 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerConsumptionPolicy

Beschreibung: Stellt Berechtigungen für den Zugriff auf die AWS License Manager Manager-API-Aktionen bereit, die für die Nutzung von Lizenzen erforderlich sind, für die der Benutzer berechtigt ist.

`AWSLicenseManagerConsumptionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSLicenseManagerConsumptionPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. August 2021, 23:18 Uhr UTC
- Bearbeitete Zeit: 11. August 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Beschreibung: Ermöglicht dem AWS License Manager Linux Subscriptions Service, Ressourcen in Ihrem Namen zu verwalten.

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Dezember 2022, 18:54 UTC
- Bearbeitete Zeit: 20. Dezember 2022, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerMasterAccountRolePolicy

Beschreibung: Rollenrichtlinie für das Masterkonto des AWS License Manager Manager-Dienstes

`AWSLicenseManagerMasterAccountRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 19:03 UTC
- Bearbeitete Zeit: 31. Mai 2022, 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerMemberAccountRolePolicy

Beschreibung: Rollenrichtlinie für Mitgliedskonten des AWS License Manager Manager-Dienstes

`AWSLicenseManagerMemberAccountRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 19:04 UTC
- Bearbeitete Zeit: 15. November 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerServiceRolePolicy

Beschreibung: Standardrollenrichtlinie für den AWS License Manager Manager-Dienst

`AWSLicenseManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 19:02 UTC
- Bearbeitete Zeit: 30. Juli 2021, 01:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPermissionsForCreatingMemberSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3BucketPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSTopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeHosts"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Beschreibung: Ermöglicht dem AWS License Manager User Subscriptions Service, Ressourcen in Ihrem Namen zu verwalten.

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. Juli 2022, 01:17 UTC
- Zeit bearbeitet: 21. November 2022, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSM2ServicePolicy

Beschreibung: Ermöglicht AWS M2, AWS Ressourcen in Ihrem Namen zu verwalten.

`AWSM2ServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Juni 2022, 20:26 UTC
- Bearbeitete Zeit: 7. Juni 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagedServices_ContactsServiceRolePolicy

Beschreibung: Ermöglicht AWS Managed Services, die Werte der Tags auf AWS Ressourcen zu lesen

`AWSManagedServices_ContactsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. März 2023, 17:07 UTC
- Bearbeitete Zeit: 23. März 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Beschreibung: AWS Managed Services — Richtlinie zur Verwaltung der Detective Controls-Infrastruktur

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Dezember 2022, 23:11 UTC
- Zeit bearbeitet: 19. Dezember 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagedServices_EventsServiceRolePolicy

Beschreibung: AWS Managed Services Services-Richtlinie zur Aktivierung der AMS-Ereignisprozessor-Funktion.

`AWSManagedServices_EventsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Februar 2023, 18:41 UTC
- Bearbeitete Zeit: 7. Februar 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagedServicesDeploymentToolkitPolicy

Beschreibung: Ermöglicht AWS Managed Services, das Deployment Toolkit in Ihrem Namen zu verwalten.

`AWSManagedServicesDeploymentToolkitPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. Juni 2022, 18:33 UTC
- Bearbeitete Zeit: 4. April 2024, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "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*"
```

```
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceAmiIngestion

Beschreibung: Ermöglicht AWS Marketplace das Kopieren Ihrer Amazon Machine Images (AMIs), um sie aufzulisten AWS Marketplace

`AWSMarketplaceAmiIngestion`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceAmiIngestion` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. September 2020, 20:55 UTC
- Bearbeitete Zeit: 25. September 2020, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceDeploymentServiceRolePolicy

Beschreibung: Ermöglicht AWS Marketplace die Erstellung und Verwaltung von Verkäufer-Deployment-Parametern für die Produkte, die Sie abonnieren AWS Marketplace.

`AWSMarketplaceDeploymentServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2023, 23:34 UTC
- Bearbeitete Zeit: 15. November 2023, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceFullAccess

Beschreibung: Ermöglicht das Abonnieren und Abbestellen von AWS Marketplace Software, ermöglicht Benutzern die Verwaltung von Marketplace-Softwareinstanzen über die Marketplace-Seite „Ihre Software“ und bietet Administratorzugriff auf EC2.

`AWSMarketplaceFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Februar 2015, 17:21 Uhr UTC
- Bearbeitete Zeit: 4. März 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
```

```
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish",
        "sns:setTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:*image-build*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
```

```
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceGetEntitlements

Beschreibung: Bietet Lesezugriff auf AWS Marketplace Berechtigungen

`AWSMarketplaceGetEntitlements`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceGetEntitlements` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. März 2017, 19:37 UTC
- Bearbeitete Zeit: 5. April 2024, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceImageBuildFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS Marketplace Private Image Build-Funktion. Neben der Erstellung privater Images bietet es auch Berechtigungen zum Hinzufügen von Tags zu Images sowie zum Starten und Beenden von EC2-Instances.

`AWSMarketplaceImageBuildFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceImageBuildFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Juli 2018, 23:29 Uhr UTC
- Bearbeitete Zeit: 4. März 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceLicenseManagementServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die AWS Marketplace für die Lizenzverwaltung verwendet oder verwaltet werden.

`AWSMarketplaceLicenseManagementServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Dezember 2020, 08:33 UTC
- Bearbeitete Zeit: 3. Dezember 2020, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceManageSubscriptions

Beschreibung: Ermöglicht das Abonnieren und Abbestellen von AWS Marketplace Software

`AWSMarketplaceManageSubscriptions`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceManageSubscriptions` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 19. Januar 2023, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceMeteringFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Marketplace Metering.

`AWSMarketplaceMeteringFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceMeteringFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. März 2016, 22:39 Uhr UTC
- Bearbeitete Zeit: 17. März 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceMeteringRegisterUsage

Beschreibung: Stellt Berechtigungen zur Registrierung einer Ressource und zur Nachverfolgung der Nutzung über den AWS Marketplace Messdienst bereit.

`AWSMarketplaceMeteringRegisterUsage`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceMeteringRegisterUsage` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. November 2019, 01:17 UTC
- Zeit bearbeitet: 21. November 2019, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceProcurementSystemAdminFullAccess

Beschreibung: Bietet vollen Zugriff auf alle administrativen Aktionen für eine AWS Marketplace eProcurement-Integration.

`AWSMarketplaceProcurementSystemAdminFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceProcurementSystemAdminFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juni 2019, 13:07 UTC
- Bearbeitete Zeit: 25. Juni 2019, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplacePurchaseOrdersServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff von AWS Marketplace Diensten auf die Bestellverwaltung.

`AWSMarketplacePurchaseOrdersServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 27. Oktober 2021, 15:12 Uhr UTC
- Bearbeitete Zeit: 27. Oktober 2021, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceRead-only

Beschreibung: Bietet die Möglichkeit, AWS Marketplace Abonnements zu überprüfen

`AWSMarketplaceRead-only`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceRead-only` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 19. Januar 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
```

```
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow"
    },
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:DescribeBuilds",
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ]
    },
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf Ressourcen AWS-Services und die Ressourcen, die von AWS Marketplace for Resale Authorization verwendet oder verwaltet werden.

`AWSMarketplaceResaleAuthorizationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. März 2024, 18:47 UTC
- Bearbeitete Zeit: 5. März 2024, 18:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "aws-marketplace:Entity"
        },
        "ArnLike" : {
          "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/
ResaleAuthorization/*"
        },
        "Null" : {
          "ram:Principal" : "true"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "Null" : {
          "ram:Principal" : "false"
        },
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAccept",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ]
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
```

```
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceSellerFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Verkäufervorgänge AWS Marketplace und andere AWS Dienste wie AMI-Management.

`AWSMarketplaceSellerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceSellerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juli 2019, 20:40 UTC
- Bearbeitete Zeit: 15. März 2024, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewMarketing",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
        "aws-marketplace-management:viewSettings",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "aws-marketplace:UpdateTask",
        "aws-marketplace:CompleteTask",
        "aws-marketplace:GetSellerDashboard",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgreementAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AssetScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsights",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "SellerSettings",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:GetSellerVerificationDetails",
        "aws-marketplace-management:PutSellerVerificationDetails",
        "aws-marketplace-management:GetBankAccountVerificationDetails",
        "aws-marketplace-management:PutBankAccountVerificationDetails",
        "aws-marketplace-management:GetSecondaryUserVerificationDetails",
        "aws-marketplace-management:PutSecondaryUserVerificationDetails",
        "aws-marketplace-management:GetAdditionalSellerNotificationRecipients",
        "aws-marketplace-management:PutAdditionalSellerNotificationRecipients",
        "payments:GetPaymentInstrument",
        "payments:CreatePaymentInstrument",
        "tax:GetTaxInterview",
        "tax:PutTaxInterview",
        "tax:GetTaxInfoReportingDocument"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Support",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourcePolicyManagement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceSellerProductsFullAccess

Beschreibung: Bietet Verkäufern vollen Zugriff auf die AWS Marketplace Management-Produktseite und andere AWS Dienste wie AMI-Management.

`AWSMarketplaceSellerProductsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceSellerProductsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juli 2019, 21:06 UTC
- Bearbeitete Zeit: 18. Juli 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "aws-marketplace:UpdateTask",
        "aws-marketplace:CompleteTask",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceSellerProductsReadOnly

Beschreibung: Bieten Sie Verkäufern nur Lesezugriff auf die Seite mit AWS Marketplace Verwaltungsprodukten.

`AWSMarketplaceSellerProductsReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMarketplaceSellerProductsReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juli 2019, 21:40 UTC
- Zeit bearbeitet: 19. November 2022, 00:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListTasks",
        "aws-marketplace:DescribeTask",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMediaConnectServicePolicy

Beschreibung: Die Standardrichtlinie, die den Zugriff AWS-Services auf Ressourcen ermöglicht, die von verwendet oder verwaltet werden MediaConnect.

`AWSMediaConnectServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 03. April 2023, 22:11 UTC
- Bearbeitete Zeit: 03. April 2023, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMediaTailorServiceRolePolicy

Beschreibung: Ermöglichen Sie den Zugriff auf AWS Ressourcen, die verwendet oder verwaltet werden von MediaTailor

`AWSMediaTailorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. September 2021, 22:27 UTC
- Bearbeitete Zeit: 17. September 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubDiscoveryAccess

Beschreibung: Die Richtlinie AWSMigrationHubService ermöglicht es, AWSApplicationDiscoveryService im Namen des Kunden anzurufen.

`AWSMigrationHubDiscoveryAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubDiscoveryAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:30 Uhr UTC
- Bearbeitete Zeit: 6. August 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubDMSAccess

Beschreibung: Richtlinie für den Database Migration Service, die Rolle im Kundenkonto zu übernehmen, um Migration Hub anzurufen

`AWSMigrationHubDMSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubDMSAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 14:00 Uhr UTC
- Bearbeitete Zeit: 7. Oktober 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubFullAccess

Beschreibung: Verwaltete Richtlinie, um dem Kunden Zugriff auf den Migration Hub Service zu gewähren

`AWSMigrationHubFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. August 2017, 14:02 UTC
- Bearbeitete Zeit: 19. Juni 2019, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubOrchestratorConsoleFullAccess

Beschreibung: Bietet eingeschränkten Zugriff auf AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service und AWS Secrets Manager. Diese Richtlinie gewährt auch vollen Zugriff auf den AWS Migration Hub Orchestrator-Dienst.

`AWSMigrationHubOrchestratorConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubOrchestratorConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 20. April 2022, 02:26 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubOrchestratorInstanceRolePolicy

Beschreibung: Diese Richtlinie muss für SAP- und MGN-migrierte Instanzen angehängt werden, damit unser Service Instanzen orchestrieren kann, indem er Skripts von S3 herunterlädt und geheime Werte innerhalb der EC2-Instanz abruft.

`AWSMigrationHubOrchestratorInstanceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubOrchestratorInstanceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 20. April 2022, 02:43 UTC
- Bearbeitete Zeit: 20. April 2022, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubOrchestratorPlugin

Beschreibung: Bietet eingeschränkten Zugriff auf Amazon Simple Storage Service, AWS Secrets Manager und Plugin-bezogene Aktionen für AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorPlugin`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubOrchestratorPlugin` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. April 2022, 02:25 UTC
- Bearbeitete Zeit: 20. April 2022, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubOrchestratorServiceRolePolicy

Beschreibung: Stellt die erforderlichen Berechtigungen für Migration Hub Orchestrator bereit, um Ihre lokalen Workloads zu migrieren und zu modernisieren

`AWSMigrationHubOrchestratorServiceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. April 2022, 02:24 UTC
- Bearbeitete Zeit: 4. März 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS Migration Hub Refactor Spaces und andere AWS zugehörige Dienste mit Ausnahme von AWS Transit Gateway- und EC2-Sicherheitsgruppen, die bei der Verwendung von Umgebungen ohne Netzwerkbrücke nicht erforderlich sind. Diese Richtlinie

schließt auch Berechtigungen aus, die für AWS Lambda und AWS Resource Access Manager erforderlich sind, da sie anhand von Tags eingeschränkt werden können.

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. April 2023, 20:09 UTC
- Bearbeitete Zeit: 11. April 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Beschreibung: Wird in der IAM-Dienstrolle verwendet, die an das SSM-Automatisierungsdokument übergeben wurde, CreateResources um AWSRefactorSpaces die für die Ausführung der Automatisierung erforderlichen Berechtigungen zu gewähren. Die Richtlinie gewährt Lese-/Schreibzugriff auf EC2-Tags, um den Automatisierungsfortschritt zu verfolgen. Wenn die Netzwerkbrücke der Refactor Spaces-Umgebung aktiviert ist, fügt die Automatisierung der EC2-Instance auch die Sicherheitsgruppe der Umgebung hinzu, um Datenverkehr von anderen Refactor Spaces-Diensten in der Umgebung zuzulassen. Die Richtlinie gewährt auch Zugriff auf die SSM-Parameter für Aktionen nach dem Start des Application Migration Service.

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. August 2023, 15:08 UTC

- Bearbeitete Zeit: 10. August 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpacesFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS MigrationHub Refactor Spaces, AWS MigrationHub Refactor Spaces-Konsolenfunktionen und andere verwandte AWS Dienste, mit Ausnahme der für AWS Lambda und AWS Resource Access Manager erforderlichen Berechtigungen, da diese basierend auf Tags eingeschränkt werden können.

`AWSMigrationHubRefactorSpacesFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubRefactorSpacesFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 07:12 UTC
- Bearbeitete Zeit: 11. April 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpacesServiceRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von AWS Migration Hub Refactor Spaces verwaltet oder verwendet werden.

`AWSMigrationHubRefactorSpacesServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2021, 06:50 UTC
- Bearbeitete Zeit: 20. Juli 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubSMSAccess

Beschreibung: Richtlinie für den Servermigrationsdienst, die Rolle im Kundenkonto zu übernehmen, um Migration Hub anzurufen

`AWSMigrationHubSMSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubSMSAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:57 UTC
- Bearbeitete Zeit: 7. Oktober 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubStrategyCollector

Beschreibung: Erteilt Berechtigungen für die Kommunikation mit dem AWS Migration Hub Strategy Recommendations Service, Lese-/Schreibzugriff auf S3-Buckets, die sich auf den Service beziehen, Amazon API Gateway Gateway-Zugriff zum Hochladen von Protokollen und Metriken AWS, AWS Secrets Manager Manager-Zugriff zum Abrufen von Anmeldeinformationen und alle zugehörigen Dienste.

`AWSMigrationHubStrategyCollector`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubStrategyCollector` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Oktober 2021, 20:15 Uhr UTC
- Bearbeitete Zeit: 1. April 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubStrategyConsoleFullAccess

Beschreibung: Gewährt vollen Zugriff auf den Service AWS Migration Hub Strategy Recommendations und Zugriff auf verwandte AWS Dienste über die AWS Management Console.

`AWSMigrationHubStrategyConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMigrationHubStrategyConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Oktober 2021, 20:13 Uhr UTC
- Bearbeitete Zeit: 9. November 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubStrategyServiceRolePolicy

Beschreibung: Ermöglichen Sie den Zugriff auf AWS Ressourcen, die vom AWS Migration Hub Strategy Recommendations Service verwendet oder verwaltet werden.

`AWSMigrationHubStrategyServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Oktober 2021, 20:02 UTC
- Bearbeitete Zeit: 19. Oktober 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMobileHub_FullAccess

Beschreibung: Diese Richtlinie kann an jeden Benutzer, jede Rolle oder Gruppe angehängt werden, um Benutzern die Erlaubnis zu erteilen, Projekte (und die zugehörigen AWS Ressourcen) in AWS Mobile Hub zu erstellen, zu löschen und zu ändern. Dazu gehören auch Berechtigungen zum

Generieren und Herunterladen von Beispielquellcode für mobile Apps für jedes Mobile Hub Hub-Projekt.

`AWSMobileHub_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMobileHub_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Januar 2016, 19:56 UTC
- Bearbeitete Zeit: 19. Dezember 2019, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMobileHub_ReadOnly

Beschreibung: Diese Richtlinie kann an jeden Benutzer, jede Rolle oder Gruppe angehängt werden, um Benutzern die Erlaubnis zu erteilen, Projekte in AWS Mobile Hub aufzulisten und anzusehen. Dazu gehören auch Berechtigungen zum Generieren und Herunterladen von Beispielquellcode für mobile Apps für jedes Mobile Hub Hub-Projekt. Es erlaubt dem Benutzer nicht, die Konfiguration für ein Mobile Hub Hub-Projekt zu ändern.

`AWSMobileHub_ReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMobileHub_ReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Januar 2016, 19:55 UTC
- Bearbeitete Zeit: 23. Juli 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMSKReplicatorExecutionRole

Beschreibung: Erteilt Amazon MSK Replicator die Erlaubnis, Daten zwischen MSK-Clustern zu replizieren.

`AWSMSKReplicatorExecutionRole`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSMSKReplicatorExecutionRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Dezember 2023, 00:07 Uhr UTC
- Bearbeitete Zeit: 25. März 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkFirewallServiceRolePolicy

Beschreibung: Ermöglicht AWSNetworkFirewall die Erstellung und Verwaltung der erforderlichen Ressourcen für Ihre Firewalls.

`AWSNetworkFirewallServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. November 2020, 17:17 Uhr UTC
- Bearbeitete Zeit: 30. März 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkManagerCloudWANServiceRolePolicy

Beschreibung: Erlauben Sie NetworkManager den Zugriff auf Ressourcen, die mit Ihrem Kernnetzwerk verknüpft sind

`AWSNetworkManagerCloudWANServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juli 2022, 12:17 UTC
- Bearbeitete Zeit: 12. Juli 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkManagerFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon NetworkManager über die AWS Management Console.

`AWSNetworkManagerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSNetworkManagerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 17:37 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkManagerReadOnlyAccess

Beschreibung: Bietet Nur-Lesezugriff auf Amazon NetworkManager über die AWS Management Console.

`AWSNetworkManagerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSNetworkManagerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 17:35 Uhr UTC
- Bearbeitete Zeit: 3. Dezember 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkManagerServiceRolePolicy

Beschreibung: Erlauben Sie den NetworkManager Zugriff auf Ressourcen, die Ihren globalen Netzwerken zugeordnet sind

`AWSNetworkManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Dezember 2019, 14:03 UTC
- Bearbeitete Zeit: 27. Juli 2022, 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOpsWorks_FullAccess

Beschreibung: Bietet vollen Zugriff auf AWS OpsWorks.

`AWSOpsWorks_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOpsWorks_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. Januar 2021, 16:29 UTC

- Bearbeitete Zeit: 22. Januar 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorks_FullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "iam:ListUsers",
        "opsworks:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "opsworks.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOpsWorksCloudWatchLogs

Beschreibung: Ermöglicht OpsWorks Instanzen, für die die CWLogs-Integration aktiviert ist, Logs zu versenden und die erforderlichen Log-Gruppen zu erstellen

`AWSOpsWorksCloudWatchLogs`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOpsWorksCloudWatchLogs` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. März 2017, 17:47 Uhr UTC

- Bearbeitete Zeit: 30. März 2017, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCloudWatchLogs`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOpsWorksCMInstanceProfileRole

Beschreibung: Bietet S3-Zugriff für von OpsWorks CM gestartete Instances.

`AWSOpsWorksCMInstanceProfileRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOpsWorksCMInstanceProfileRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. November 2016, 09:48 UTC
- Bearbeitete Zeit: 23. April 2021, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksCMInstanceProfileRole`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      ]
    },
    {
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-opsworks-cm-*",
      "Effect" : "Allow"
    },
    {
      "Action" : "acm:GetCertificate",
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOpsWorksCMServiceRole

Beschreibung: Service Role Policy, die für die Erstellung von OpsWorks CM-Servern verwendet werden soll.

`AWSOpsWorksCMServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOpsWorksCMServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. November 2016, 09:49 UTC
- Bearbeitete Zeit: 23. April 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSOpsWorksCMServiceRole`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
```

```
        "s3:PutObject",
        "s3:GetBucketTagging",
        "s3:PutBucketTagging"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "tag:UntagResources",
        "tag:TagResources"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
        }
      },
      "Action" : [
        "ssm:SendCommand"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
```

```
        "arn:aws:ssm:*::document/*",
        "arn:aws:s3:::aws-opsworks-cm-*"
      ],
      "Action" : [
        "ssm:SendCommand"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateImage",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RunInstances",
        "ec2:StopInstances"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-opsworks-cm-*"
        }
      },
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:RebootInstances"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:opsworks-cm:*:*:server/*"
      ],
      "Action" : [
        "opsworks-cm:DeleteServer",
        "opsworks-cm:StartMaintenance"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/aws-opsworks-cm-*"
      ],
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-opsworks-cm-*",
        "arn:aws:iam::*:role/service-role/aws-opsworks-cm-*"
      ],
      "Action" : [
        "iam:PassRole"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Resource" : "*",
      "Action" : [
        "acm:DeleteCertificate",
        "acm:ImportCertificate"
      ]
    },
    {
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:opsworks-cm!aws-opsworks-cm-secrets-*",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOpsWorksInstanceRegistration

Beschreibung: Ermöglicht den Zugriff für eine Amazon EC2 EC2-Instance zur Registrierung bei einem AWS OpsWorks Stack.

`AWSOpsWorksInstanceRegistration`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOpsWorksInstanceRegistration` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Juni 2016, 14:23 Uhr UTC
- Bearbeitete Zeit: 3. Juni 2016, 14:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:RegisterInstance"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOpsWorksRegisterCLI_EC2

Beschreibung: Richtlinie zur Aktivierung der Registrierung von EC2-Instances über die CLI OpsWorks

`AWSOpsWorksRegisterCLI_EC2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOpsWorksRegisterCLI_EC2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juni 2019, 15:56 UTC
- Bearbeitete Zeit: 18. Juni 2019, 15:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_EC2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOpsWorksRegisterCLI_OnPremises

Beschreibung: Richtlinie zur Aktivierung der Registrierung von On-Premises-Instanzen über die CLI OpsWorks

`AWSOpsWorksRegisterCLI_OnPremises`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOpsWorksRegisterCLI_OnPremises` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juni 2019, 15:33 UTC
- Bearbeitete Zeit: 18. Juni 2019, 15:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOpsWorksRegisterCLI_OnPremises`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
      "Effect" : "Allow",
      "Action" : [
        "opsworks:AssignInstance",
        "opsworks:CreateLayer",
        "opsworks:DeregisterInstance",
        "opsworks:DescribeInstances",
        "opsworks:DescribeStackProvisioningParameters",
        "opsworks:DescribeStacks",
        "opsworks:UnassignInstance"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateGroup",
        "iam:AddUserToGroup"
      ],
      "Resource" : [
        "arn:aws:iam::*:group/AWS/OpsWorks/OpsWorks-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateUser",
        "iam:CreateAccessKey"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/AWS/OpsWorks/OpsWorks-*"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSOpsWorksInstanceRegistration"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOrganizationsFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Organizations.

`AWSOrganizationsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOrganizationsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. November 2018, 20:31 UTC

- Bearbeitete Zeit: 6. Februar 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOrganizationsReadOnlyAccess

Beschreibung: Bietet Nur-Lese-Zugriff für Organizations. AWS

`AWSOrganizationsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOrganizationsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. November 2018, 20:32 UTC
- Bearbeitete Zeit: 7. Juni 2024, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOrganizationsServiceTrustPolicy

Beschreibung: Eine Richtlinie, die es AWS Organizations ermöglicht, Vertrauen mit anderen zu teilen, die genehmigt wurde AWS-Services , um die Kundenkonfiguration zu vereinfachen.

`AWSOrganizationsServiceTrustPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Oktober 2017, 23:04 UTC
- Bearbeitete Zeit: 1. November 2017, 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOutpostsAuthorizeServerPolicy

Beschreibung: Diese Richtlinie gewährt Ihnen Berechtigungen, mit denen Sie einen Outpost-Server in Ihrem lokalen Netzwerk installieren können.

`AWSOutpostsAuthorizeServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSOutpostsAuthorizeServerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Januar 2023, 19:23 UTC
- Bearbeitete Zeit: 4. Januar 2023, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOutpostsServiceRolePolicy

Beschreibung: Richtlinie für dienstverknüpfte Rollen, um den Zugriff auf AWS Ressourcen zu ermöglichen, die von AWS Outposts verwaltet werden

`AWSOutpostsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. November 2020, 22:55 UTC
- Zeit bearbeitet: 9. November 2020, 22:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaApplianceRolePolicy

Beschreibung: Ermöglicht der AWS IoT-Software auf einer AWS Panorama-Appliance, Protokolle auf Amazon hochzuladen CloudWatch.

`AWSPanoramaApplianceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPanoramaApplianceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 1. Dezember 2020, 13:13 Uhr UTC
- Zeit bearbeitet: 1. Dezember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaApplianceServiceRolePolicy

Beschreibung: Ermöglicht einer AWS Panorama-Appliance CloudWatch, Protokolle auf Amazon hochzuladen und Objekte von Amazon S3 S3-Zugriffspunkten abzurufen, die für die Verwendung mit AWS Panorama erstellt wurden.

`AWSPanoramaApplianceServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPanoramaApplianceServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. Oktober 2021, 12:14 Uhr UTC
- Bearbeitete Zeit: 17. Januar 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*-nodepackage-store-*",
        "arn:aws:s3:::*-application-payload-store-*",
        "arn:aws:s3:*:*:accesspoint/panorama*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Panorama

`AWSPanoramaFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPanoramaFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 1. Dezember 2020, 13:12 UTC
- Bearbeitete Zeit: 12. Januar 2022, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "panorama.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "panorama.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaGreengrassGroupRolePolicy

Beschreibung: Ermöglicht einer AWS Lambda-Funktion auf einer AWS Panorama-Appliance, Ressourcen in Panorama zu verwalten, Protokolle und Metriken auf Amazon hochzuladen und Objekte in Buckets zu verwalten CloudWatch, die für die Verwendung mit Panorama erstellt wurden.

`AWSPanoramaGreengrassGroupRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPanoramaGreengrassGroupRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2020, 13:10 Uhr UTC
- Bearbeitete Zeit: 6. Januar 2021, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaSageMakerRolePolicy

Beschreibung: Ermöglicht Amazon SageMaker , Objekte in Buckets zu verwalten, die für die Verwendung mit AWS Panorama erstellt wurden.

`AWSPanoramaSageMakerRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPanoramaSageMakerRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2020, 13:13 Uhr UTC
- Zeit bearbeitet: 1. Dezember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaServiceLinkedRolePolicy

Beschreibung: Ermöglicht AWS Panorama die Verwaltung von Ressourcen in AWS IoT, AWS Secrets Manager und AWS Panorama.

`AWSPanoramaServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Oktober 2021, 12:12 Uhr UTC
- Bearbeitete Zeit: 20. Oktober 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaServiceRolePolicy

Beschreibung: Ermöglicht AWS Panorama, Ressourcen in Amazon S3, AWS IoT, AWS IoT GreenGrass, AWS Lambda SageMaker, Amazon und Amazon CloudWatch Logs zu verwalten und Servicerollen an AWS IoT GreenGrass, AWS IoT und Amazon SageMaker zu übergeben.

`AWSPanoramaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPanoramaServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2020, 13:14 Uhr UTC
- Zeit bearbeitet: 1. Dezember 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPriceListServiceFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Preislistenservice.

`AWSPriceListServiceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPriceListServiceFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. November 2017, 00:36 UTC
- Zeit bearbeitet: 22. November 2017, 00:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAAuditor

Beschreibung: Bietet Auditor-Zugriff auf die AWS private Zertifizierungsstelle

`AWSPrivateCAAuditor`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPrivateCAAuditor` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:33 UTC

- Bearbeitete Zeit: 14. Februar 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS private Zertifizierungsstelle

`AWSPrivateCAFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPrivateCAFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:20 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAPrivilegedUser

Beschreibung: Bietet privilegierten Zertifikatsbenutzern Zugriff auf die AWS Private Certificate Authority

`AWSPrivateCAPrivilegedUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPrivateCAPrivilegedUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:26 UTC

- Bearbeitete Zeit: 14. Februar 2023, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/*CACertificate*/V*"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS private Zertifizierungsstelle

`AWSPrivateCAReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPrivateCAReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:30 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAUser

Beschreibung: Ermöglicht Zertifikatsbenutzern Zugriff auf die AWS private Zertifizierungsstelle

`AWSPrivateCAUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPrivateCAUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:16 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "StringNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateMarketplaceAdminFullAccess

Beschreibung: Bietet vollen Zugriff auf alle administrativen Aktionen für einen AWS privaten Marketplace.

`AWSPrivateMarketplaceAdminFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPrivateMarketplaceAdminFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 16:32 UTC
- Bearbeitete Zeit: 14. Februar 2024, 22:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceRequestPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogTaggingPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateMarketplaceRequests

Beschreibung: Ermöglicht den Zugriff auf die Erstellung von Anfragen auf einem AWS privaten Marketplace.

`AWSPrivateMarketplaceRequests`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPrivateMarketplaceRequests` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Oktober 2019, 21:44 Uhr UTC
- Bearbeitete Zeit: 28. Oktober 2019, 21:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateNetworksServiceRolePolicy

Beschreibung: Ermöglicht AWS Private Networks Service, Ressourcen im Namen des Kunden zu verwalten.

`AWSPrivateNetworksServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Dezember 2021, 23:17 Uhr UTC
- Bearbeitete Zeit: 16. Dezember 2021, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonCodeBuildProvisioningBasicAccess

Beschreibung: Permissions CodeBuild benötigt, um einen Build für AWS Proton CodeBuild Provisioning auszuführen.

`AWSProtonCodeBuildProvisioningBasicAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSProtonCodeBuildProvisioningBasicAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. November 2022, 21:04 UTC
- Zeit bearbeitet: 9. November 2022, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonCodeBuildProvisioningServiceRolePolicy

Beschreibung: Ermöglicht AWS Proton, die Bereitstellung von Proton-Ressourcen mithilfe CodeBuild und anderer AWS Dienste in Ihrem Namen zu verwalten.

`AWSProtonCodeBuildProvisioningServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. November 2022, 21:32 UTC
- Bearbeitete Zeit: 17. Mai 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonDeveloperAccess

Beschreibung: Bietet Zugriff auf die AWS Proton-APIs und die Management Console, ermöglicht jedoch keine Verwaltung von Proton-Vorlagen oder -Umgebungen.

`AWSProtonDeveloperAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSProtonDeveloperAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Februar 2021, 19:02 UTC
- Bearbeitungszeit: 6. Juni 2024, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS Proton-APIs und die Management Console. Zusätzlich zu diesen Berechtigungen ist Zugriff auf Amazon S3 erforderlich, um Vorlagenpakete aus Ihren S3-Buckets zu registrieren, sowie Zugriff auf Amazon IAM, um die Servicerollen für Proton zu erstellen und zu verwalten.

`AWSProtonFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSProtonFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Februar 2021, 19:07 UTC
- Bearbeitungszeit: 6. Juni 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS Proton-APIs und die Management Console.

`AWSProtonReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSProtonReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Februar 2021, 19:09 UTC
- Zeit bearbeitet: 18. November 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonServiceGitSyncServiceRolePolicy

Beschreibung: Richtlinie, die es AWS Proton ermöglicht, Ihre Service-, Umgebungs- und Komponentendefinitionen aus Ihrem Git-Repository mit AWS Proton zu synchronisieren.

`AWSProtonServiceGitSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. April 2023, 15:55 UTC
- Bearbeitete Zeit: 4. April 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonSyncServiceRolePolicy

Beschreibung: Richtlinie, die es AWS Proton ermöglicht, den Inhalt Ihres Git-Repositorys mit Proton zu synchronisieren oder Proton-Inhalte mit Ihren Git-Repositorys zu synchronisieren.

`AWSProtonSyncServiceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. November 2021, 21:14 UTC
- Bearbeitete Zeit: 5. Mai 2024, 01:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPurchaseOrdersServiceRolePolicy

Beschreibung: Erteilt Berechtigungen zum Anzeigen und Ändern von Bestellungen in der Abrechnungskonsole

`AWSPurchaseOrdersServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSPurchaseOrdersServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Mai 2020, 18:15 UTC
- Bearbeitete Zeit: 17. Juli 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "aws-portal:*Billing",
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "payments:GetPaymentInstrument",
        "payments:ListPaymentPreferences",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
```

```
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightAssetBundleExportPolicy

Beschreibung: Stellt die Berechtigungen bereit, die für die Ausführung von QuickSight Asset Bundle-Exportvorgängen erforderlich sind

`AWSQuickSightAssetBundleExportPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightAssetBundleExportPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 27. März 2024, 21:31 UTC
- Bearbeitete Zeit: 27. März 2024, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightAssetBundleImportPolicy

Beschreibung: Stellt die Berechtigungen bereit, die für die Durchführung von QuickSight Asset-Bundle-Importvorgängen erforderlich sind

`AWSQuickSightAssetBundleImportPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightAssetBundleImportPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. März 2024, 21:40 UTC
- Bearbeitete Zeit: 27. März 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuicksightAthenaAccess

Beschreibung: Quicksight-Zugriff auf die Athena-API und S3-Buckets, die für Athena-Abfrageergebnisse verwendet werden

`AWSQuicksightAthenaAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuicksightAthenaAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 9. Dezember 2016, 02:31 UTC
- Bearbeitete Zeit: 7. Juli 2021, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightDescribeRDS

Beschreibung: QuickSight Erlaubt die Beschreibung der RDS-Ressourcen

`AWSQuickSightDescribeRDS`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightDescribeRDS` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 10. November 2015, 23:24 Uhr UTC
- Zeit bearbeitet: 10. November 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightDescribeRedshift

Beschreibung: Erlaubt QuickSight die Beschreibung von Redshift-Ressourcen

`AWSQuickSightDescribeRedshift`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightDescribeRedshift` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. November 2015, 23:25 Uhr UTC
- Zeit bearbeitet: 10. November 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightElasticsearchPolicy

Beschreibung: Bietet Zugriff auf Amazon Elasticsearch-Ressourcen von Amazon QuickSight

`AWSQuickSightElasticsearchPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightElasticsearchPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. September 2020, 17:27 UTC
- Bearbeitete Zeit: 7. September 2021, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightIoTAnalyticsAccess

Beschreibung: Geben Sie QuickSight schreibgeschützten Zugriff auf IoT Analytics Analytics-Datensätze

`AWSQuickSightIoTAnalyticsAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightIoTAnalyticsAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 17:00 Uhr UTC
- Zeit bearbeitet: 29. November 2017, 17:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightListIAM

Beschreibung: Erlaubt QuickSight das Auflisten von IAM-Entitäten

`AWSQuickSightListIAM`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightListIAM` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. November 2015, 23:25 Uhr UTC
- Zeit bearbeitet: 10. November 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuicksightOpenSearchPolicy

Beschreibung: Bietet Zugriff auf OpenSearch Amazon-Ressourcen von Amazon QuickSight

`AWSQuicksightOpenSearchPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuicksightOpenSearchPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. September 2021, 23:26 UTC
- Bearbeitete Zeit: 7. September 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightSageMakerPolicy

Beschreibung: Bietet Zugriff auf SageMaker Amazon-Ressourcen von Amazon QuickSight

`AWSQuickSightSageMakerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightSageMakerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. Januar 2020, 17:18 Uhr UTC
- Bearbeitete Zeit: 30. Oktober 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightTimestreamPolicy

Beschreibung: AWS QuickSight Zugriff auf AWS Timestream-APIs. Kunden können diese Richtlinie an AWS QuickSight eine Rolle anhängen, um das Abrufen von Daten und Metadaten zu ermöglichen.

`AWSQuickSightTimestreamPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSQuickSightTimestreamPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 30. September 2020, 21:47 Uhr UTC
- Bearbeitete Zeit: 30. September 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSReachabilityAnalyzerServiceRolePolicy

Beschreibung: Ermöglicht VPC Reachability Analyzer den Zugriff auf AWS Ressourcen und die Integration mit AWS Organizations in Ihrem Namen.

`AWSReachabilityAnalyzerServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. November 2022, 17:12 UTC
- Bearbeitete Zeit: 15. Mai 2024, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReachabilityAnalyzerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
```

```
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
```

```
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApigatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRefactoringToolkitFullAccess

Beschreibung: Diese Richtlinie gewährt die Erlaubnis zur Nutzung von AWS Diensten mit der AWS Toolkit for .NET Refactoring-Erweiterung für Microsoft Visual Studio. Sie soll an ein lokales Profil angehängt werden. AWS Die Richtlinie ermöglicht das Hochladen von Anwendungsartefakten und das Herunterladen der resultierenden Artefakte von Amazon S3. Es ermöglicht das Erstellen von Anwendungen in einem Container-Image mithilfe AWS CodeBuild und Speichern und Abrufen der Images aus Amazon Elastic Container Registry (Amazon ECR). Und es ermöglicht die Bereitstellung der Anwendung für Container-Services AWS wie Amazon Elastic Container Service (Amazon ECS), die optionale Erstellung von VPC-Ressourcen, die optionale Verbindung zu vorhandener Infrastruktur wie AWS Directory Service und andere verwandte Dienste.

`AWSRefactoringToolkitFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSRefactoringToolkitFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Oktober 2022, 16:41 UTC
- Bearbeitete Zeit: 25. März 2024, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "App2ContainerAccess",
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Sid" : "CodeBuildCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "CodeBuildExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
    {
      "Sid" : "CreateSecurityGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2CreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2CreateAccessATS",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2ModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2ModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcrCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "EcrModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcrModifyAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
```

```
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcsCreateAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsModifyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "EcsModifyAccessATS",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcsReadTaskDefinitionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EcsExecuteCommandInSidecar",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Sid" : "EcsExecuteCommandInSidecarATS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
    },
    {
      "Sid" : "CreateEcsServiceLinkedRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "a2c-generated"
          ]
        }
      }
    },
    {
      "Sid" : "CloudwatchCreateAccessATS",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "application-transformation"
          ]
        }
      }
    },
    {
      "Sid" : "CloudwatchGetAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Sid" : "CloudwatchGetAccessATS",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "SsmParameterAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
```

```
      ]
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
          ]
        }
      }
    },
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "clouddirectory:ListDirectories",
        "codebuild:BatchGetProjects",
        "codebuild:BatchGetBuilds",
        "ds:DescribeDirectories",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ecr:DescribeImages",
        "ecr:DescribeRepositories",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTasks",
```

```
        "ecs:ListTagsForResource",
        "ecs:ListTasks",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetECSSLR",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
    {
      "Sid" : "PortingAssistantFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
    {
      "Sid" : "ApplicationTransformationAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment",
        "application-transformation:PutLogData",
        "application-transformation:PutMetricData",
        "application-transformation:StartContainerization",
        "application-transformation:GetContainerization",
        "application-transformation:StartDeployment",
        "application-transformation:GetDeployment"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    },
    {
      "Sid" : "EcrPushAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "ecr:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Sid" : "EcrAuthAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRefactoringToolkitSidecarPolicy

Beschreibung: Diese Richtlinie ist für Amazon ECS-Aufgaben vorgesehen, die zum Testen von Anwendungen AWS mithilfe der AWS Toolkit for .NET Refactoring-Erweiterung für Microsoft Visual Studio erstellt wurden. Die Richtlinie gewährt Zugriff auf das Herunterladen von Anwendungsartefakten von Amazon S3, die Übermittlung des Status der Aufgabe mithilfe von AWS Systems Manager und andere erforderliche Dienste.

`AWSRefactoringToolkitSidecarPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSRefactoringToolkitSidecarPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Oktober 2022, 16:41 UTC
- Zeit bearbeitet: 29. Oktober 2022, 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSrePostPrivateCloudWatchAccess

Beschreibung: Bietet re:POST Private-Zugriff zum Veröffentlichen CloudWatch von Metrikdaten

`AWSrePostPrivateCloudWatchAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2023, 16:37 UTC
- Bearbeitete Zeit: 15. November 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRepostSpaceSupportOperationsPolicy

Beschreibung: Diese Richtlinie ermöglicht es dem re:POST Space-Dienst, Supportanfragen zu erstellen, zu verwalten und zu lösen, die über die Space-Anwendung erstellt wurden.

`AWSRepostSpaceSupportOperationsPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSRepostSpaceSupportOperationsPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. November 2023, 21:52 UTC
- Bearbeitete Zeit: 26. November 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResilienceHubAsssessmentExecutionPolicy

Beschreibung: Richtlinie für die AWS Resilience Hub-Dienstrolle, die den Zugriff auf andere AWS Dienste ermöglicht, um die Bewertung durchzuführen.

`AWSResilienceHubAsssessmentExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResilienceHubAsssessmentExecutionPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2023, 12:32 UTC
- Bearbeitete Zeit: 24. März 2024, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
```

```
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
```

```
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3Statement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
```

```
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*"
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "ResilienceHub"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubSSMStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceAccessManagerFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Resource Access Manager

`AWSResourceAccessManagerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResourceAccessManagerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Juni 2019, 17:28 UTC
- Bearbeitete Zeit: 4. Juni 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceAccessManagerReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Resource Access Manager.

`AWSResourceAccessManagerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResourceAccessManagerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Dezember 2019, 20:58 UTC
- Bearbeitete Zeit: 9. Dezember 2019, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  "Statement" : [
    {
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceAccessManagerResourceShareParticipantAccess

Beschreibung: Bietet Zugriff auf AWS Resource Access Manager Manager-APIs, die von einem Resource Share-Teilnehmer benötigt werden.

`AWSResourceAccessManagerResourceShareParticipantAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResourceAccessManagerResourceShareParticipantAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Dezember 2019, 20:41 UTC
- Bearbeitete Zeit: 9. Dezember 2019, 20:41 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceAccessManagerServiceRolePolicy

Beschreibung: Richtlinie, die den schreibgeschützten AWS Resource Access Manager auf die Organisationsstruktur der Kunden vorsieht. Sie enthält auch IAM-Berechtigungen für das eigenständige Löschen der Rolle.

`AWSResourceAccessManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2018, 19:28 UTC
- Zeit bearbeitet: 14. November 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerFullAccess

Beschreibung: Diese Richtlinie gewährt Administratorberechtigungen für den Zugriff auf Resource Explorer-Ressourcen und gewährt anderen AWS Diensten zur Unterstützung dieses Zugriffs nur Leseberechtigungen.

`AWSResourceExplorerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResourceExplorerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. November 2022, 20:01 UTC
- Bearbeitete Zeit: 14. November 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerOrganizationsAccess

Beschreibung: Diese Richtlinie gewährt Resource Explorer Administratorberechtigungen und anderen AWS Diensten zur Unterstützung dieses Zugriffs nur Leseberechtigungen. Der AWS Organisationsadministrator benötigt diese Berechtigungen, um die Suche mit mehreren Konten in der Konsole einzurichten und zu verwalten.

`AWSResourceExplorerOrganizationsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResourceExplorerOrganizationsAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. November 2023, 17:01 UTC
- Bearbeitete Zeit: 14. November 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Leseberechtigungen zum Suchen und Anzeigen von Resource Explorer-Ressourcen und gewährt anderen AWS Diensten zur Unterstützung dieses Zugriffs nur Leseberechtigungen.

`AWSResourceExplorerReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResourceExplorerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. November 2022, 19:56 UTC
- Bearbeitete Zeit: 14. November 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerServiceRolePolicy

Beschreibung: Ermöglicht Resource Explorer, Ressourcen und CloudTrail Ereignisse in Ihrem Namen anzuzeigen, um Ihre Ressourcen für die Suche zu indizieren.

`AWSResourceExplorerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Oktober 2022, 20:35 UTC
- Bearbeitete Zeit: 20. Dezember 2023, 13:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-explorer-2/*"
      ]
    },
    {
```

```
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/deployments"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "amplify:ListApps",
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplifyuibuilder:ListComponents",
        "amplifyuibuilder:ListThemes",
        "app-integrations:ListEventIntegrations",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appsync:ListGraphqlApis",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListWorkspaces",
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListReportPlans",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:ListSchedulingPolicies",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudfront:ListCachePolicies",
```

```
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "codeartifact:ListDomains",
        "codeartifact:ListRepositories",
        "codebuild:ListProjects",
        "codecommit:ListRepositories",
        "codeguru-profiler:ListProfilingGroups",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "databrew:ListDatasets",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "detective:ListGraphs",
        "ds:DescribeDirectories",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
```

```
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpams",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstances",
```

```
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSubnetCidrReservations",
        "ecr:DescribeRepositories",
        "ecr-public:DescribeRepositories",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "emr-serverless:ListApplications",
        "es:ListDomainNames",
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
```

```
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
        "fis:ListExperimentTemplates",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetLabels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "gamelift:ListAliases",
        "geo:ListPlaceIndexes",
        "geo:ListTrackers",
        "greengrass:ListComponents",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:GetDatabases",
        "glue:GetJobs",
        "glue:GetTables",
        "glue:GetTriggers",
        "greengrass:ListComponentVersions",
        "greengrass:ListGroups",
        "healthlake:ListFHIRDatastores",
        "iam:ListGroups",
        "iam:ListInstanceProfiles",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
```

```
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iot:ListJobTemplates",
        "iot:ListAuthorizers",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListSecurityProfiles",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListWorkspaces",
        "kafka:ListConfigurations",
        "kms:ListKeys",
        "ivs:ListChannels",
        "ivs:ListStreamKeys",
        "kafka:ListClusters",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListStreams",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
```

```
        "lookoutmetrics:ListAlerts",
        "lookoutvision:ListProjects",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mq:ListBrokers",
        "mediatailor:ListPlaybackConfigurations",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "panorama:ListPackages",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
```

```
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeReservedDBInstances",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverRules",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListStorageLensConfigurations",
        "sagemaker:ListModels",
        "sagemaker:ListNotebookInstances",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAttributeGroups",
```

```
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeParameters",
        "ssm:DescribePatchBaselines",
        "ssm-incidents:ListResponsePlans",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListInventoryEntries",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "timestream:ListDatabases",
        "wisdom:listAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:listKnowledgeBases"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceGroupsReadOnlyAccess

Beschreibung: Dies ist die schreibgeschützte Richtlinie für AWS Resource Groups

`AWSResourceGroupsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSResourceGroupsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. März 2018, 10:27 UTC
- Bearbeitete Zeit: 5. Februar 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRoboMaker_FullAccess

Beschreibung: Bietet vollen Zugriff auf AWS RoboMaker über das AWS Management Console und SDK. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, IAM).

`AWSRoboMaker_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSRoboMaker_FullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. September 2020, 18:34 UTC
- Bearbeitete Zeit: 16. September 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRoboMakerReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS RoboMaker über das AWS Management Console und SDK

`AWSRoboMakerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSRoboMakerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. November 2018, 05:30 Uhr UTC
- Bearbeitete Zeit: 28. August 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRoboMakerServicePolicy

Beschreibung: RoboMaker Servicerichtlinie

`AWSRoboMakerServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 06:30 Uhr UTC
- Bearbeitete Zeit: 11. November 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRoboMakerServiceRolePolicy

Beschreibung: RoboMaker Servicerichtlinie

`AWSRoboMakerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSRoboMakerServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. November 2018, 05:33 UTC
- Bearbeitete Zeit: 26. November 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRolesAnywhereServicePolicy

Beschreibung: Ermöglicht es IAM Roles Anywhere, Service/Nutzungs-Metriken an private Zertifizierungsstellen zu veröffentlichen CloudWatch und deren Status in Ihrem Namen zu überprüfen.

`AWSRolesAnywhereServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Juli 2022, 15:26 UTC
- Bearbeitete Zeit: 5. Juli 2022, 15:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSS3OnOutpostsServiceRolePolicy

Beschreibung: Erlauben Sie dem Amazon S3 on Outposts-Service, EC2-Netzwerkressourcen in Ihrem Namen zu verwalten.

`AWSS3OnOutpostsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Oktober 2023, 20:32 UTC
- Bearbeitete Zeit: 3. Oktober 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSavingsPlansFullAccess

Beschreibung: Bietet vollen Zugriff auf den Savings Plans-Service

`AWSSavingsPlansFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSavingsPlansFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. November 2019, 22:45 UTC
- Bearbeitete Zeit: 6. November 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSavingsPlansReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Savings Plans-Service

`AWSSavingsPlansReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSavingsPlansReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. November 2019, 22:45 UTC
- Bearbeitete Zeit: 6. November 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubFullAccess

Beschreibung: Bietet vollen Zugriff auf die Nutzung von AWS Security Hub.

`AWSSecurityHubFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSecurityHubFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 23:54 UTC
- Bearbeitete Zeit: 23. April 2024, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "inspector2:BatchGetAccountStatus",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubOrganizationsAccess

Beschreibung: Erteilt die Erlaubnis, AWS Security Hub innerhalb einer Organisation zu aktivieren und zu verwalten. Beinhaltet die unternehmensweite Aktivierung des Dienstes und die Festlegung des delegierten Administratorkontos für den Dienst.

`AWSSecurityHubOrganizationsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSecurityHubOrganizationsAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. März 2021, 20:53 UTC
- Bearbeitete Zeit: 16. November 2023, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securityhub.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Security Hub Hub-Ressourcen

`AWSSecurityHubReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSecurityHubReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 01:34 UTC
- Bearbeitete Zeit: 22. Februar 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubServiceRolePolicy

Beschreibung: Eine dienstbezogene Rolle, die AWS Security Hub benötigt, um auf Ihre Ressourcen zugreifen zu können.

`AWSSecurityHubServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. November 2018, 23:47 UTC
- Bearbeitete Zeit: 27. November 2023, 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAdminFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltungsfunktionen des Servicekatalogs

`AWSServiceCatalogAdminFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSServiceCatalogAdminFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Februar 2018, 17:19 Uhr UTC
- Bearbeitete Zeit: 13. April 2023, 18:43 UTC

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

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAdminReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die Administratorfunktionen von Service Catalog

`AWSServiceCatalogAdminReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSServiceCatalogAdminReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Oktober 2019, 18:53 Uhr UTC
- Bearbeitete Zeit: 25. Oktober 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAppRegistryFullAccess

Beschreibung: Bietet vollen Zugriff auf die Funktionen der Service Catalog App Registry

`AWSServiceCatalogAppRegistryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSServiceCatalogAppRegistryFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. November 2020, 22:25 UTC
- Bearbeitete Zeit: 7. Dezember 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAppRegistryReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die Funktionen der Service Catalog App Registry

`AWSServiceCatalogAppRegistryReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSServiceCatalogAppRegistryReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. November 2020, 22:34 UTC

- Zeit bearbeitet: 17. November 2022, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAppRegistryServiceRolePolicy

Beschreibung: Ermöglicht Service Catalog AppRegistry , Resource Groups in Ihrem Namen zu verwalten

`AWSServiceCatalogAppRegistryServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. Mai 2021, 22:18 Uhr UTC
- Bearbeitete Zeit: 26. Oktober 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogEndUserFullAccess

Beschreibung: Bietet vollen Zugriff auf die Funktionen des Servicekatalogs für Endbenutzer

`AWSServiceCatalogEndUserFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSServiceCatalogEndUserFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Februar 2018, 17:22 Uhr UTC
- Bearbeitete Zeit: 10. Juli 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogEndUserReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Service Catalog-Endbenutzerfunktionen

`AWSServiceCatalogEndUserReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSServiceCatalogEndUserReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Oktober 2019, 18:49 UTC
- Bearbeitete Zeit: 25. Oktober 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Beschreibung: Eine serviceverknüpfte Rollenrichtlinie AWS ServiceCatalog zur Synchronisierung mit der Organisationsstruktur von AWS Organizations

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. April 2023, 20:48 UTC
- Bearbeitete Zeit: 10. April 2023, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
```

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogSyncServiceRolePolicy

Beschreibung: Eine serviceverknüpfte Rolle AWS ServiceCatalog zum Synchronisieren von Bereitstellungsartefakten aus Quell-Repositorys

`AWSServiceCatalogSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2022, 21:20 UTC
- Bearbeitete Zeit: 03. Mai 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForAmazonEKSNodegroup

Beschreibung: Erforderliche Berechtigungen für die Verwaltung von Knotengruppen im Kundenkonto. Diese Richtlinien betrafen die Verwaltung der folgenden Ressourcen: AutoscalingGroups, SecurityGroups, LaunchTemplates und. InstanceProfiles

`AWSServiceRoleForAmazonEKSNodegroup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. November 2019, 01:34 UTC
- Zeit bearbeitet: 4. Januar 2024, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
```

```
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
    },
    {
      "Sid" : "AllowAutoscalingToCreateSLR",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      },
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowASGCreationByEKS",
      "Effect" : "Allow",
      "Action" : [
```

```
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToManageResourcesForNodegroups",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "ec2:CreateLaunchTemplate",
```

```
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "ec2:DescribeLaunchTemplates",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RunInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:GetConsoleOutput",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
    },
    {
      "Sid" : "PermissionsToManageEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForAmazonQDeveloper

Beschreibung: Diese serviceverknüpfte Rolle bietet Amazon Q Developer die Möglichkeit, Nutzungsinformationen bereitzustellen.

`AWSServiceRoleForAmazonQDeveloper`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. April 2024, 07:40 UTC
- Bearbeitete Zeit: 25. April 2024, 07:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

Beschreibung: Bietet Zugriff auf Systems Manager Manager-Ressourcen, die von CloudWatch Alarms verwendet werden

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Oktober 2020, 09:49 UTC
- Zeit bearbeitet: 1. Oktober 2020, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

Beschreibung: Ermöglicht CloudWatch den Zugriff auf RDS Performance Insights Insights-Metriken in Ihrem Namen

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. September 2023, 09:32 UTC
- Bearbeitete Zeit: 7. September 2023, 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCodeGuru-Profiler

Beschreibung: Eine servicebezogene Rolle, die Amazon CodeGuru Profiler benötigt, um Benachrichtigungen in Ihrem Namen zu versenden.

`AWSServiceRoleForCodeGuru-Profiler`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. Juni 2020, 22:04 UTC
- Bearbeitete Zeit: 26. Juni 2020, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCodeWhispererPolicy

Beschreibung: Diese Rolle gewährt Berechtigungen für den CodeWhisperer Zugriff auf Daten in Ihrem Konto, um die Abrechnung zu berechnen, bietet Zugriff auf die Erstellung und den Zugriff auf Sicherheitsberichte in Amazon CodeGuru sowie die Übermittlung von Daten an CloudWatch.

`AWSServiceRoleForCodeWhispererPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. März 2023, 19:39 UTC
- Bearbeitete Zeit: 29. März 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForEC2ScheduledInstances

Beschreibung: Ermöglicht EC2 Scheduled Instances das Starten und Verwalten von Spot-Instances.

`AWSServiceRoleForEC2ScheduledInstances`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Oktober 2017, 18:31 Uhr UTC
- Zeit bearbeitet: 12. Oktober 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Beschreibung: AWS GroundStation verwendet diese dienstbezogene Rolle, um EC2 aufzurufen, um öffentliche IPv4-Adressen zu finden

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Dezember 2022, 23:52 UTC
- Bearbeitete Zeit: 13. Dezember 2022, 23:52 UTC

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

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForImageBuilder

Beschreibung: Ermöglicht EC2ImageBuilder , AWS Dienste in Ihrem Namen aufzurufen.

`AWSServiceRoleForImageBuilder`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2019, 22:02 UTC
- Bearbeitete Zeit: 19. Oktober 2023, 21:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Version der Richtlinie

Richtlinienversion: v19 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
```

```
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateLaunchTemplate",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeSnapshots",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateImage"
          ],
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListInventoryEntries",
        "ssm:SendAutomationSignal",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:DescribeAssociationExecutions",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:StartAutomationExecution",
      "Resource" : "arn:aws:ssm:*:*:automation-definition/ImageBuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
```

```
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
```

```
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForIoTSiteWise

Beschreibung: Ermöglicht AWS IoT SiteWise die Bereitstellung und Verwaltung von Gateways sowie die Abfrage von Daten. Die Richtlinie umfasst die erforderlichen AWS Greengrass-Berechtigungen für die Bereitstellung in Gruppen, AWS Lambda-Berechtigungen für die Erstellung und Aktualisierung von Funktionen mit Servicepräfix und AWS IoT Analytics Analytics-Berechtigungen für die Abfrage von Daten aus Datenspeichern.

`AWSServiceRoleForIoTSiteWise`AWS ist eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2018, 19:19 UTC
- Bearbeitete Zeit: 13. November 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForLogDeliveryPolicy

Beschreibung: Ermöglicht dem Log Delivery Service, Protokolle zu übermitteln, indem er das Protokollziel in Ihrem Namen anruft.

`AWSServiceRoleForLogDeliveryPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. Oktober 2019, 17:31 UTC
- Bearbeitete Zeit: 15. Juli 2021, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForMonitronPolicy

Beschreibung: Erteilt Amazon Monitron Berechtigungen zur Verwaltung von AWS Ressourcen, einschließlich der AWS SSO-Benutzerzuweisung in Ihrem Namen.

`AWSServiceRoleForMonitronPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Dezember 2020, 19:06 UTC
- Bearbeitete Zeit: 29. September 2022, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:ListDirectoryAssociations",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForNeptuneGraphPolicy

Beschreibung: Bietet Cloudwatch-Zugriff zur Veröffentlichung von Betriebs- und Nutzungsmetriken und Protokollen für Amazon Neptune

`AWSServiceRoleForNeptuneGraphPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2023, 14:03 UTC
- Bearbeitete Zeit: 29. November 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Beschreibung: Bietet Berechtigungen zur Beschreibung und Aktualisierung von Private Marketplace-Ressourcen und zur Beschreibung von AWS Organizations

`AWSServiceRoleForPrivateMarketplaceAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. Februar 2024, 22:28 UTC
- Bearbeitete Zeit: 14. Februar 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForSMS

Beschreibung: Bietet Zugriff auf AWS Dienste und Ressourcen, die für die Migration von Dienstinstanzen in AWS EC2, S3 und Cloudformation erforderlich sind.

`AWSServiceRoleForSMS`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. August 2019, 18:39 Uhr UTC

- Bearbeitete Zeit: 15. Oktober 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForUserSubscriptions

Beschreibung: Ermöglicht den Zugriff auf Ihre Identity Center-Ressourcen über den Service Benutzerabonnements, um Ihre Abonnements automatisch zu aktualisieren.

`AWSServiceRoleForUserSubscriptions`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. April 2024, 16:14 UTC
- Bearbeitete Zeit: 25. April 2024, 16:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SubscriptionManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "organizations:DescribeOrganization",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRolePolicyForBackupReports

Beschreibung: Bietet AWS Backup-Berechtigungen zum Erstellen von Compliance-Berichten in Ihrem Namen

`AWSServiceRolePolicyForBackupReports`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. August 2021, 21:16 UTC
- Bearbeitete Zeit: 10. März 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRolePolicyForBackupRestoreTesting

Beschreibung: Diese Richtlinie enthält Berechtigungen zum Testen von Wiederherstellungen und zum Bereinigen von Ressourcen, die während der Tests erstellt wurden.

`AWSServiceRolePolicyForBackupRestoreTesting`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. November 2023, 23:37 UTC
- Bearbeitete Zeit: 14. Februar 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
        "backup:GetRecoveryPointRestoreMetadata",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByResource",
        "backup:ListTags",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:TerminateInstances",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:DeleteMountTarget",
        "rds:DeleteDBCluster",
        "rds:DeleteDBInstance",
        "fsx:DeleteFileSystem",
        "fsx:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/awsbackup-restore-test" : "false"
        }
      }
    },
    {
      "Sid" : "DdbDeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDeleteActions",
      "Effect" : "Allow",
      "Action" : "redshift:DeleteCluster",
      "Resource" : "arn:aws:redshift:*:*:cluster:awsbackup-restore-test-*"
    },
    {
```

```
      "Sid" : "S3DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TimestreamDeleteActions",
      "Effect" : "Allow",
      "Action" : "timestream:DeleteTable",
      "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSShieldDRTAccessPolicy

Beschreibung: Bietet dem AWS DDoS-Reaktionsteam eingeschränkten Zugriff auf Sie, AWS-Konto um Sie bei der Abwehr von DDoS-Angriffen bei einem Ereignis mit hohem Schweregrad zu unterstützen.

`AWSShieldDRTAccessPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSShieldDRTAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2018, 22:29 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSShieldServiceRolePolicy

Beschreibung: Ermöglicht AWS Shield, in Ihrem Namen auf AWS Ressourcen zuzugreifen, um DDoS-Schutz zu bieten.

`AWSShieldServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 17. November 2021, 19:17 UTC
- Bearbeitete Zeit: 17. November 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSMForSAPServiceLinkedRolePolicy

Beschreibung: Stellt AWS Systems Manager for SAP die Berechtigungen bereit, die für die Verwaltung und Integration von SAP-Software erforderlich sind AWS.

`AWSSSMForSAPServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. November 2022, 01:18 UTC
- Bearbeitete Zeit: 11. April 2024, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

```
        "ec2:DescribeInstances",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:*:events:*:*:rule/SSMSAPManagedRule*",
        "arn:*:events:*:*:event-bus/default"
      ]
    },
    {
      "Sid" : "DocumentActions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
        "arn:*:ssm:*:*:document/AWSSSMSAP*",
        "arn:*:ssm:*:*:document/AWSSAP*"
      ]
    },
    {
      "Sid" : "CustomerSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
```

```
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ssm:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "InstanceTagActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/awsApplication" : "false"
        },
        "StringEqualsIgnoreCase" : {
          "ec2:ResourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "DescribeTag",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeTags",
      "Resource" : "*"
    },
    {
      "Sid" : "GetApplication",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetApplication",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "UpdateOrDeleteApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DeleteApplication",
        "servicecatalog:UpdateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TagResource",
        "servicecatalog:CreateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:*:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
```

```
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
```

```
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    },
    {
      "Sid" : "StartStopInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
```

```
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSMOpsInsightsServiceRolePolicy

Beschreibung: Richtlinie für die Rolle „Service Linked“ AWSServiceRoleForAmazonSSM_OpsInsights

`AWSSSMOpsInsightsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Juni 2021, 20:12 UTC
- Bearbeitete Zeit: 16. Juni 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSODirectoryAdministrator

Beschreibung: Administratorzugriff für das SSO-Verzeichnis

`AWSSSODirectoryAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSSODirectoryAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Oktober 2018, 23:54 UTC
- Bearbeitete Zeit: 20. Oktober 2022, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
```

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSODirectoryReadOnly

Beschreibung: ReadOnly Zugriff auf das SSO-Verzeichnis

`AWSSSODirectoryReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSSODirectoryReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Oktober 2018, 23:49 UTC
- Zeit bearbeitet: 16. November 2022, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSOMasterAccountAdministrator

Beschreibung: Bietet Zugriff innerhalb von AWS SSO zur Verwaltung der Master- und Mitgliedskonten von AWS Organizations sowie der Cloud-Anwendung

`AWSSSOMasterAccountAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSSOMasterAccountAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2018, 20:36 UTC
- Bearbeitete Zeit: 26. April 2024, 00:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSOMemberAccountAdministrator

Beschreibung: Bietet Zugriff innerhalb von AWS SSO zur Verwaltung von Mitgliedskonten und Cloud-Anwendungen von AWS Organizations

`AWSSSOMemberAccountAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSSOMemberAccountAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2018, 20:45 UTC
- Bearbeitete Zeit: 26. April 2024, 00:31 UTC

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

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSOReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS SSO-Konfigurationen.

`AWSSSOReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSSOReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2018, 20:24 UTC
- Bearbeitete Zeit: 26. April 2024, 00:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSOServiceRolePolicy

Beschreibung: Gewährt AWS SSO-Berechtigungen zur Verwaltung von AWS Ressourcen, einschließlich IAM-Rollen, Richtlinien und SAML-IdP, in Ihrem Namen.

`AWSSSOServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Dezember 2017, 18:36 Uhr UTC
- Bearbeitete Zeit: 20. Oktober 2022, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v17 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


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

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStepFunctionsConsoleFullAccess

Beschreibung: Eine Zugriffsrichtlinie, um einem Benutzer/einer Rolle/usw. Zugriff auf die Konsole zu gewähren. AWS StepFunctions Für ein vollständiges Konsolenerlebnis benötigt ein Benutzer zusätzlich zu dieser Richtlinie möglicherweise die iam: PassRole -Berechtigung für andere IAM-Rollen, die vom Dienst übernommen werden können.

`AWSStepFunctionsConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSStepFunctionsConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Januar 2017, 21:54 UTC
- Zeit bearbeitet: 12. Januar 2017, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStepFunctionsFullAccess

Beschreibung: Eine Zugriffsrichtlinie, um einem Benutzer/einer Rolle/usw. Zugriff auf die API zu gewähren. AWS StepFunctions Um vollen Zugriff zu erhalten, MUSS ein Benutzer zusätzlich zu dieser Richtlinie über die iam: PassRole -Berechtigung für mindestens eine IAM-Rolle verfügen, die vom Dienst übernommen werden kann.

`AWSStepFunctionsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSStepFunctionsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Januar 2017, 21:51 UTC

- Zeit bearbeitet: 11. Januar 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStepFunctionsReadOnlyAccess

Beschreibung: Eine Zugriffsrichtlinie, mit der einem Benutzer/einer Rolle/usw. nur Lesezugriff auf den Dienst gewährt werden kann. AWS StepFunctions

`AWSStepFunctionsReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSStepFunctionsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Januar 2017, 21:46 Uhr UTC
- Bearbeitete Zeit: 26. April 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

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

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStorageGatewayFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Storage Gateway über die AWS Management Console.

`AWSStorageGatewayFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSStorageGatewayFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. September 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStorageGatewayReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf AWS Storage Gateway über die AWS Management Console.

`AWSStorageGatewayReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSStorageGatewayReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. September 2022, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStorageGatewayServiceRolePolicy

Beschreibung: Dienstbezogene Rolle, die von AWS Storage Gateway verwendet wird, um die Integration anderer AWS Dienste mit Storage Gateway zu ermöglichen.

`AWSStorageGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Februar 2021, 19:03 UTC
- Bearbeitete Zeit: 17. Februar 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupplyChainFederationAdminAccess

Beschreibung: AWSSupplyChainFederationAdminAccess bietet Verbundbenutzern von AWS Supply Chain Zugriff auf die AWS Supply Chain-Anwendung, einschließlich der erforderlichen Berechtigungen, um Aktionen innerhalb der AWS Supply-Chain-Anwendung auszuführen. Die Richtlinie gewährt Administratorberechtigungen für Benutzer und Gruppen von IAM Identity Center und ist einer Rolle zugeordnet, die von AWS Supply Chain in Ihrem Namen erstellt wurde. Sie sollten keine AWSSupplyChainFederationAdminAccess Richtlinie an andere IAM-Entitäten anhängen.

`AWSSupplyChainFederationAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSupplyChainFederationAdminAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. März 2023, 18:54 UTC
- Bearbeitete Zeit: 1. November 2023, 18:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime:DeleteChannelMembership",
        "chime:DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
      ],
      "Resource" : [
```

```
        "arn:aws:chime:*:*:app-instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SCNInstanceId" : "*"
        }
      }
    },
    {
      "Sid" : "ChimeChannel",
      "Effect" : "Allow",
      "Action" : [
        "chime:DescribeChannel"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ]
    },
    {
      "Sid" : "ChimeMessaging",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMessagingSessionEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:ListDirectoryAssociations",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppflowConnectorProfile",
      "Effect" : "Allow",
      "Action" : [
```

```
        "appflow:CreateConnectorProfile",
        "appflow:UseConnectorProfile",
        "appflow:DeleteConnectorProfile",
        "appflow:UpdateConnectorProfile"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:connectorprofile/scn-*"
      ]
    },
    {
      "Sid" : "AppflowFlow",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateFlow",
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow",
        "appflow:TagResource",
        "appflow:UntagResource"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:flow/scn-*"
      ]
    },
    {
      "Sid" : "S3ListAllBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListSupplyChainBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ]
    },
    {
      "Sid" : "S3ReadWriteObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "KMSListKeys",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSListGrants",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportAccess

Beschreibung: Ermöglicht Benutzern den Zugriff auf das AWS Support Center.

`AWSSupportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSupportAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportAppFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS Support App und andere erforderliche Dienste wie AWS Support Service Quotas. Diese Richtlinie beinhaltet Berechtigungen zur Nutzung der unterstützenden Dienste, sodass sich der Benutzer bei AWS Support Supportanfragen an sie wenden, Servicekontingente ändern und die entsprechenden dienstbezogenen Rollen erstellen kann.

`AWSSupportAppFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSupportAppFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. August 2022, 16:53 UTC
- Bearbeitete Zeit: 22. August 2022, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportAppReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS Support App.

`AWSSupportAppReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSupportAppReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 22. August 2022, 17:01 UTC
- Bearbeitete Zeit: 22. August 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportPlansFullAccess

Beschreibung: Bietet vollen Zugriff auf Supportpläne.

`AWSSupportPlansFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSupportPlansFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. September 2022, 18:19 UTC
- Bearbeitete Zeit: 9. Mai 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportPlansReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Supportpläne.

`AWSSupportPlansReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSupportPlansReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. September 2022, 18:08 UTC
- Bearbeitete Zeit: 27. September 2022, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportServiceRolePolicy

Beschreibung: Ermöglicht AWS Support den Zugriff auf AWS Ressourcen zur Bereitstellung von Abrechnungs-, Verwaltungs- und Supportdiensten.

`AWSSupportServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. April 2018, 18:04 UTC
- Bearbeitete Zeit: 02. Mai 2024, 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v36 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
```

```
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Action" : [
        "iam:DeleteRole"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActions",
      "Action" : [
        "access-analyzer:getAccessPreview",
        "access-analyzer:getAnalyzedResource",
        "access-analyzer:getAnalyzer",
        "access-analyzer:getArchiveRule",
        "access-analyzer:getFinding",
        "access-analyzer:getGeneratedPolicy",
        "access-analyzer:listAccessPreviewFindings",
        "access-analyzer:listAccessPreviews",
        "access-analyzer:listAnalyzedResources",
        "access-analyzer:listAnalyzers",
        "access-analyzer:listArchiveRules",
        "access-analyzer:listFindings",
        "access-analyzer:listPolicyGenerations",
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "airflow:getEnvironment",
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
        "amplify:listApps",
```

```
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "appflow:describeConnectorEntity",
        "appflow:describeConnectorProfiles",
        "appflow:describeConnectors",
        "appflow:describeFlow",
        "appflow:describeFlowExecutionRecords",
        "appflow:listConnectorEntities",
        "appflow:listFlows",
        "application-autoscaling:describeScalableTargets",
        "application-autoscaling:describeScalingActivities",
        "application-autoscaling:describeScalingPolicies",
        "application-autoscaling:describeScheduledActions",
        "applicationinsights:describeApplication",
        "applicationinsights:describeComponent",
        "applicationinsights:describeComponentConfiguration",
        "applicationinsights:describeComponentConfigurationRecommendation",
        "applicationinsights:describeLogPattern",
        "applicationinsights:describeObservation",
        "applicationinsights:describeProblem",
        "applicationinsights:describeProblemObservations",
        "applicationinsights:listApplications",
        "applicationinsights:listComponents",
        "applicationinsights:listConfigurationHistory",
        "applicationinsights:listLogPatterns",
        "applicationinsights:listLogPatternSets",
        "applicationinsights:listProblems",
        "appmesh:describeGatewayRoute",
        "appmesh:describeMesh",
        "appmesh:describeRoute",
        "appmesh:describeVirtualGateway",
        "appmesh:describeVirtualNode",
        "appmesh:describeVirtualRouter",
        "appmesh:describeVirtualService",
        "appmesh:listGatewayRoutes",
        "appmesh:listMeshes",
        "appmesh:listRoutes",
        "appmesh:listTagsForResource",
        "appmesh:listVirtualGateways",
        "appmesh:listVirtualNodes",
```

```
        "appmesh:listVirtualRouters",
        "appmesh:listVirtualServices",
        "apprunner:describeAutoScalingConfiguration",
        "apprunner:describeCustomDomains",
        "apprunner:describeOperation",
        "apprunner:describeService",
        "apprunner:listAutoScalingConfigurations",
        "apprunner:listConnections",
        "apprunner:listOperations",
        "apprunner:listServices",
        "apprunner:listTagsForResource",
        "appstream:describeAppBlockBuilderAppBlockAssociations",
        "appstream:describeAppBlockBuilders",
        "appstream:describeAppBlocks",
        "appstream:describeApplicationFleetAssociations",
        "appstream:describeApplications",
        "appstream:describeDirectoryConfigs",
        "appstream:describeEntitlements",
        "appstream:describeFleets",
        "appstream:describeImageBuilders",
        "appstream:describeImagePermissions",
        "appstream:describeImages",
        "appstream:describeSessions",
        "appstream:describeStacks",
        "appstream:describeUsageReportSubscriptions",
        "appstream:describeUsers",
        "appstream:describeUserStackAssociations",
        "appstream:listAssociatedFleets",
        "appstream:listAssociatedStacks",
        "appstream:listEntitledApplications",
        "appstream:listTagsForResource",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listDataSources",
        "appsync:listDomainNames",
        "appsync:listFunctions",
```

```
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
        "aps:describeRuleGroupsNamespace",
        "aps:describeScraper",
        "aps:describeWorkspace",
        "aps:listRuleGroupsNamespaces",
        "aps:listScrapers",
        "aps:listWorkspaces",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "auditmanager:getAccountStatus",
        "auditmanager:getDelegations",
        "auditmanager:listAssessmentFrameworks",
        "auditmanager:listAssessmentReports",
        "auditmanager:listAssessments",
        "auditmanager:listControls",
        "auditmanager:listKeywordsForDataSource",
```

```
        "auditmanager:listNotifications",
        "autoscaling-plans:describeScalingPlanResources",
        "autoscaling-plans:describeScalingPlans",
        "autoscaling-plans:getScalingPlanResourceForecastData",
        "autoscaling:describeAccountLimits",
        "autoscaling:describeAdjustmentTypes",
        "autoscaling:describeAutoScalingGroups",
        "autoscaling:describeAutoScalingInstances",
        "autoscaling:describeAutoScalingNotificationTypes",
        "autoscaling:describeInstanceRefreshes",
        "autoscaling:describeLaunchConfigurations",
        "autoscaling:describeLifecycleHooks",
        "autoscaling:describeLifecycleHookTypes",
        "autoscaling:describeLoadBalancers",
        "autoscaling:describeLoadBalancerTargetGroups",
        "autoscaling:describeMetricCollectionTypes",
        "autoscaling:describeNotificationConfigurations",
        "autoscaling:describePolicies",
        "autoscaling:describeScalingActivities",
        "autoscaling:describeScalingProcessTypes",
        "autoscaling:describeScheduledActions",
        "autoscaling:describeTags",
        "autoscaling:describeTerminationPolicyTypes",
        "autoscaling:describeWarmPool",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRestoreJobMetadata",
```

```
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "batch:describeComputeEnvironments",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:listJobs",
        "braket:getDevice",
        "braket:getQuantumTask",
        "braket:searchDevices",
        "braket:searchQuantumTasks",
        "budgets:viewBudget",
        "ce:getCostAndUsage",
        "ce:getCostAndUsageWithResources",
        "ce:getCostForecast",
```

```
        "ce:getDimensionValues",
        "ce:getReservationCoverage",
        "ce:getReservationPurchaseRecommendation",
        "ce:getReservationUtilization",
        "ce:getRightsizingRecommendation",
        "ce:getSavingsPlansCoverage",
        "ce:getSavingsPlansPurchaseRecommendation",
        "ce:getSavingsPlansUtilization",
        "ce:getSavingsPlansUtilizationDetails",
        "ce:getTags",
        "chime:describeAppInstance",
        "chime:getAttendee",
        "chime:getGlobalSettings",
        "chime:getMediaCapturePipeline",
        "chime:getMediaPipeline",
        "chime:getMeeting",
        "chime:getProxySession",
        "chime:getSipMediaApplication",
        "chime:getSipRule",
        "chime:getVoiceConnector",
        "chime:getVoiceConnectorGroup",
        "chime:getVoiceConnectorLoggingConfiguration",
        "chime:listAppInstances",
        "chime:listAttendees",
        "chime:listChannelBans",
        "chime:listChannels",
        "chime:listChannelsModeratedByAppInstanceUser",
        "chime:listMediaCapturePipelines",
        "chime:listMediaPipelines",
        "chime:listMeetings",
        "chime:listSipMediaApplications",
        "chime:listSipRules",
        "chime:listVoiceConnectorGroups",
        "chime:listVoiceConnectors",
        "cleanrooms:batchGetCollaborationAnalysisTemplate",
        "cleanrooms:batchGetSchema",
        "cleanrooms:getAnalysisTemplate",
        "cleanrooms:getCollaboration",
        "cleanrooms:getCollaborationAnalysisTemplate",
        "cleanrooms:getConfiguredTable",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getSchema",
        "cleanrooms:listAnalysisTemplates",
```

```
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredTableAssociations",
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listSchemas",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
```

```
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudhsm:describeBackups",
        "cloudhsm:describeClusters",
        "cloudsearch:describeAnalysisSchemes",
```

```
        "cloudsearch:describeAvailabilityOptions",
        "cloudsearch:describeDomains",
        "cloudsearch:describeExpressions",
        "cloudsearch:describeIndexFields",
        "cloudsearch:describeScalingParameters",
        "cloudsearch:describeServiceAccessPolicies",
        "cloudsearch:describeSuggesters",
        "cloudsearch:listDomainNames",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:getInsightSelectors",
        "cloudtrail:getTrail",
        "cloudtrail:getTrailStatus",
        "cloudtrail:listPublicKeys",
        "cloudtrail:listTags",
        "cloudtrail:listTrails",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
        "cloudwatch:listMetricStreams",
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
        "codebuild:batchGetBuildBatches",
```

```
        "codebuild:batchGetBuilds",
        "codebuild:batchGetFleets",
        "codebuild:batchGetProjects",
        "codebuild:listBuildBatches",
        "codebuild:listBuildBatchesForProject",
        "codebuild:listBuilds",
        "codebuild:listBuildsForProject",
        "codebuild:listCuratedEnvironmentImages",
        "codebuild:listFleets",
        "codebuild:listProjects",
        "codebuild:listSourceCredentials",
        "codecommit:batchGetRepositories",
        "codecommit:getBranch",
        "codecommit:getRepository",
        "codecommit:getRepositoryTriggers",
        "codecommit:listBranches",
        "codecommit:listRepositories",
        "codedeploy:batchGetApplicationRevisions",
        "codedeploy:batchGetApplications",
        "codedeploy:batchGetDeploymentGroups",
        "codedeploy:batchGetDeploymentInstances",
        "codedeploy:batchGetDeployments",
        "codedeploy:batchGetDeploymentTargets",
        "codedeploy:batchGetOnPremisesInstances",
        "codedeploy:getApplication",
        "codedeploy:getApplicationRevision",
        "codedeploy:getDeployment",
        "codedeploy:getDeploymentConfig",
        "codedeploy:getDeploymentGroup",
        "codedeploy:getDeploymentInstance",
        "codedeploy:getDeploymentTarget",
        "codedeploy:getOnPremisesInstance",
        "codedeploy:listApplicationRevisions",
        "codedeploy:listApplications",
        "codedeploy:listDeploymentConfigs",
        "codedeploy:listDeploymentGroups",
        "codedeploy:listDeploymentInstances",
        "codedeploy:listDeployments",
        "codedeploy:listDeploymentTargets",
        "codedeploy:listGitHubAccountTokenNames",
        "codedeploy:listOnPremisesInstances",
        "codepipeline:getJobDetails",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineExecution",
```

```
        "codepipeline:getPipelineState",
        "codepipeline:listActionExecutions",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "codepipeline:listWebhooks",
        "codestar:describeProject",
        "codestar:listProjects",
        "codestar:listResources",
        "codestar:listTeamMembers",
        "codestar:listUserProfiles",
        "codestar-connections:getConnection",
        "codestar-connections:getHost",
        "codestar-connections:listConnections",
        "codestar-connections:listHosts",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
```

```
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
        "comprehend:listSentimentDetectionJobs",
        "comprehend:listTargetedSentimentDetectionJobs",
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getEnrollmentStatus",
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
```

```
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
        "config:getComplianceDetailsByConfigRule",
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
```

```
            "connect:listRoutingProfiles",
            "connect:listSecurityProfiles",
            "connect:listUsers",
            "connect:listViews",
            "connect:listViewVersions",
            "controltower:describeAccountFactoryConfig",
            "controltower:describeCoreService",
            "controltower:describeGuardrail",
            "controltower:describeGuardrailForTarget",
            "controltower:describeManagedAccount",
            "controltower:describeSingleSignOn",
            "controltower:getAvailableUpdates",
            "controltower:getHomeRegion",
            "controltower:getLandingZone",
            "controltower:getLandingZoneStatus",
            "controltower:listDirectoryGroups",
            "controltower:listEnabledControls",
            "controltower:listGuardrailsForTarget",
            "controltower:listGuardrailViolations",
            "controltower:listLandingZones",
            "controltower:listManagedAccounts",
            "controltower:listManagedAccountsForGuardrail",
            "controltower:listManagedAccountsForParent",
            "controltower:listManagedOrganizationalUnits",
            "controltower:listManagedOrganizationalUnitsForGuardrail",
            "cost-optimization-hub:getPreferences",
            "cost-optimization-hub:getRecommendation",
            "cost-optimization-hub:listEnrollmentStatuses",
            "cost-optimization-hub:listRecommendations",
            "cost-optimization-hub:listRecommendationSummaries",
            "databrew:describeDataset",
            "databrew:describeJob",
            "databrew:describeProject",
            "databrew:describeRecipe",
            "databrew:listDatasets",
            "databrew:listJobRuns",
            "databrew:listJobs",
            "databrew:listProjects",
            "databrew:listRecipes",
            "databrew:listRecipeVersions",
            "databrew:listTagsForResource",
            "datapipeline:describeObjects",
            "datapipeline:describePipelines",
            "datapipeline:getPipelineDefinition",
```

```
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationEfs",
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOpenZfs",
        "datasync:describeLocationFsxWindows",
        "datasync:describeLocationHdfs",
        "datasync:describeLocationNfs",
        "datasync:describeLocationObjectStorage",
        "datasync:describeLocationS3",
        "datasync:describeLocationSmb",
        "datasync:describeTask",
        "datasync:describeTaskExecution",
        "datasync:listAgents",
        "datasync:listLocations",
        "datasync:listTaskExecutions",
        "datasync:listTasks",
        "dax:describeClusters",
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
        "detective:getMembers",
        "detective:listGraphs",
        "detective:listInvitations",
        "detective:listMembers",
        "devicefarm:getAccountSettings",
        "devicefarm:getDevice",
        "devicefarm:getDevicePool",
        "devicefarm:getDevicePoolCompatibility",
        "devicefarm:getJob",
        "devicefarm:getProject",
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
```

```
        "devicefarm:listJobs",
        "devicefarm:listProjects",
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "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:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
```

```
        "ds:listTagsForResource",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTimeToLive",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
```

```
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
```

```
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
```

```
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
```

```
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImages",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImageScanFindings",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:listImages",
        "ecr:listTagsForResource",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
```

```
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
```

```
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
```

```
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elastictranscoder:listJobsByPipeline",
        "elastictranscoder:listJobsByStatus",
        "elastictranscoder:listPipelines",
        "elastictranscoder:listPresets",
        "elastictranscoder:readPipeline",
        "elastictranscoder:readPreset",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
```

```
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "evidently:getExperiment",
        "evidently:getFeature",
        "evidently:getLaunch",
        "evidently:getProject",
        "evidently:getSegment",
        "evidently:listExperiments",
        "evidently:listFeatures",
        "evidently:listLaunches",
        "evidently:listProjects",
        "evidently:listSegments",
        "evidently:listSegmentReferences",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listArchives",
        "events:listApiDestinations",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
```

```
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fms:getAdminAccount",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:listComplianceStatus",
        "fms:listMemberAccounts",
        "fms:listPolicies",
        "forecast:describeDataset",
        "forecast:describeDatasetGroup",
        "forecast:describeDatasetImportJob",
        "forecast:describeForecast",
        "forecast:describeForecastExportJob",
        "forecast:describePredictor",
        "forecast:getAccuracyMetrics",
        "forecast:listDatasetGroups",
        "forecast:listDatasetImportJobs",
        "forecast:listDatasets",
        "forecast:listForecastExportJobs",
        "forecast:listForecasts",
        "forecast:listPredictors",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
```

```
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
```

```
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
```

```
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:querySchemaVersionMetadata",
        "grafana:describeWorkspace",
        "grafana:describeWorkspaceAuthentication",
        "grafana:listPermissions",
        "grafana:listVersions",
        "grafana:listWorkspaces",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
        "greengrass:getCoreDefinitionVersion",
        "greengrass:getDeploymentStatus",
        "greengrass:getDeviceDefinition",
        "greengrass:getDeviceDefinitionVersion",
        "greengrass:getFunctionDefinition",
        "greengrass:getFunctionDefinitionVersion",
        "greengrass:getGroup",
        "greengrass:getGroupCertificateAuthority",
        "greengrass:getGroupVersion",
```

```
        "greengrass:getLoggerDefinition",
        "greengrass:getLoggerDefinitionVersion",
        "greengrass:getResourceDefinitionVersion",
        "greengrass:getServiceRoleForAccount",
        "greengrass:getSubscriptionDefinition",
        "greengrass:getSubscriptionDefinitionVersion",
        "greengrass:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listDeployments",
        "greengrass:listDeviceDefinitions",
        "greengrass:listDeviceDefinitionVersions",
        "greengrass:listFunctionDefinitions",
        "greengrass:listFunctionDefinitionVersions",
        "greengrass:listGroups",
        "greengrass:listGroupVersions",
        "greengrass:listLoggerDefinitions",
        "greengrass:listLoggerDefinitionVersions",
        "greengrass:listResourceDefinitions",
        "greengrass:listResourceDefinitionVersions",
        "greengrass:listSubscriptionDefinitions",
        "greengrass:listSubscriptionDefinitionVersions",
        "guardduty:getDetector",
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMasterAccount",
        "guardduty:getMembers",
        "guardduty:getThreatIntelSet",
        "guardduty:listDetectors",
        "guardduty:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
```

```
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
```

```
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder:getDistributionConfiguration",
        "imagebuilder:getImage",
        "imagebuilder:getImagePipeline",
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflow",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listWorkflowBuildVersions",
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflows",
        "imagebuilder:listWorkflowStepExecutions",
        "imagebuilder:listTagsForResource",
        "inspector:describeAssessmentRuns",
        "inspector:describeAssessmentTargets",
        "inspector:describeAssessmentTemplates",
```

```
        "inspector:describeCrossAccountAccessRole",
        "inspector:describeResourceGroups",
        "inspector:describeRulesPackages",
        "inspector:getTelemetryMetadata",
        "inspector:listAssessmentRunAgents",
        "inspector:listAssessmentRuns",
        "inspector:listAssessmentTargets",
        "inspector:listAssessmentTemplates",
        "inspector:listEventSubscriptions",
        "inspector:listRulesPackages",
        "inspector:listTagsForResource",
        "inspector2:batchGetAccountStatus",
        "inspector2:batchGetFreeTrialInfo",
        "inspector2:describeOrganizationConfiguration",
        "inspector2:getDelegatedAdminAccount",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCisScanConfigurations",
        "inspector2:listCisScanResultsAggregatedByChecks",
        "inspector2:listCisScanResultsAggregatedByTargetResource",
        "inspector2:listCisScans",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "inspector-scan:scanSbom",
        "internetmonitor:getMonitor",
        "internetmonitor:listMonitors",
        "internetmonitor:getHealthEvent",
        "internetmonitor:listHealthEvents",
        "iot:describeAuthorizer",
        "iot:describeCACertificate",
        "iot:describeCertificate",
        "iot:describeDefaultAuthorizer",
        "iot:describeDomainConfiguration",
        "iot:describeEndpoint",
        "iot:describeIndex",
        "iot:describeJobExecution",
        "iot:describeThing",
        "iot:describeThingGroup",
        "iot:describeTunnel",
        "iot:getEffectivePolicies",
```

```
        "iot:getIndexingConfiguration",
        "iot:getLoggingOptions",
        "iot:getPolicy",
        "iot:getPolicyVersion",
        "iot:getTopicRule",
        "iot:getV2LoggingOptions",
        "iot:listAttachedPolicies",
        "iot:listAuthorizers",
        "iot:listCACertificates",
        "iot:listCertificates",
        "iot:listCertificatesByCA",
        "iot:listDomainConfigurations",
        "iot:listJobExecutionsForJob",
        "iot:listJobExecutionsForThing",
        "iot:listJobs",
        "iot:listNamedShadowsForThing",
        "iot:listOutgoingCertificates",
        "iot:listPackages",
        "iot:listPackageVersions",
        "iot:listPolicies",
        "iot:listPolicyPrincipals",
        "iot:listPolicyVersions",
        "iot:listPrincipalPolicies",
        "iot:listPrincipalThings",
        "iot:listRoleAliases",
        "iot:listTargetsForPolicy",
        "iot:listThingGroups",
        "iot:listThingGroupsForThing",
        "iot:listThingPrincipals",
        "iot:listThingRegistrationTasks",
        "iot:listThings",
        "iot:listThingsInThingGroup",
        "iot:listThingTypes",
        "iot:listTopicRules",
        "iot:listTunnels",
        "iot:listV2LoggingLevels",
        "iotevents:describeDetector",
        "iotevents:describeDetectorModel",
        "iotevents:describeInput",
        "iotevents:describeLoggingOptions",
        "iotevents:listDetectorModels",
        "iotevents:listDetectorModelVersions",
        "iotevents:listDetectors",
        "iotevents:listInputs",
```

```
        "iotfleetwise:getCampaign",
        "iotfleetwise:getDecoderManifest",
        "iotfleetwise:getFleet",
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getVehicle",
        "iotfleetwise:getVehicleStatus",
        "iotfleetwise:listCampaigns",
        "iotfleetwise:listDecoderManifests",
        "iotfleetwise:listDecoderManifestNetworkInterfaces",
        "iotfleetwise:listDecoderManifestSignals",
        "iotfleetwise:listFleets",
        "iotfleetwise:listFleetsForVehicle",
        "iotfleetwise:listModelManifests",
        "iotfleetwise:listModelManifestNodes",
        "iotfleetwise:listSignalCatalogs",
        "iotfleetwise:listSignalCatalogNodes",
        "iotfleetwise:listVehicles",
        "iotsitewise:describeAccessPolicy",
        "iotsitewise:describeAsset",
        "iotsitewise:describeAssetModel",
        "iotsitewise:describeAssetProperty",
        "iotsitewise:describeDashboard",
        "iotsitewise:describeGateway",
        "iotsitewise:describeGatewayCapabilityConfiguration",
        "iotsitewise:describeLoggingOptions",
        "iotsitewise:describePortal",
        "iotsitewise:describeProject",
        "iotsitewise:listAccessPolicies",
        "iotsitewise:listAssetModels",
        "iotsitewise:listAssets",
        "iotsitewise:listAssociatedAssets",
        "iotsitewise:listDashboards",
        "iotsitewise:listGateways",
        "iotsitewise:listPortals",
        "iotsitewise:listProjectAssets",
        "iotsitewise:listProjects",
        "iottwinmaker:getComponentType",
        "iottwinmaker:getEntity",
        "iottwinmaker:getPricingPlan",
        "iottwinmaker:getScene",
        "iottwinmaker:getWorkspace",
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
```

```
        "iottwinmaker:listScenes",
        "iottwinmaker:getSyncJob",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeVpcConnection",
```

```
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listConfigurations",
        "kafka:listConfigurationRevisions",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeDataSource",
        "kendra:describeFaq",
        "kendra:describeIndex",
        "kendra:listDataSources",
        "kendra:listFaqs",
        "kendra:listIndices",
        "kinesis:describeStream",
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
        "kinesis:listShards",
        "kinesis:listStreams",
        "kinesis:listStreamConsumers",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisvideo:describeImageGenerationConfiguration",
        "kinesisvideo:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
```

```
        "kinesisvideo:listStreams",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "lambda:listLayers",
        "lambda:listLayerVersions",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listProvisionedApps",
        "lex:describeBot",
        "lex:describeBotAlias",
        "lex:describeBotLocale",
        "lex:describeBotRecommendation",
        "lex:describeBotVersion",
```

```
        "lex:describeCustomVocabularyMetadata",
        "lex:describeExport",
        "lex:describeImport",
        "lex:describeIntent",
        "lex:describeResourcePolicy",
        "lex:describeSlot",
        "lex:describeSlotType",
        "lex:getBot",
        "lex:getBotAlias",
        "lex:getBotAliases",
        "lex:getBotChannelAssociation",
        "lex:getBotChannelAssociations",
        "lex:getBots",
        "lex:getBotVersions",
        "lex:getBuiltinIntent",
        "lex:getBuiltinIntents",
        "lex:getBuiltinSlotTypes",
        "lex:getIntent",
        "lex:getIntents",
        "lex:getIntentVersions",
        "lex:getSlotType",
        "lex:getSlotTypes",
        "lex:getSlotTypeVersions",
        "lex:listBotAliases",
        "lex:listBotLocales",
        "lex:listBotRecommendations",
        "lex:listBots",
        "lex:listBotVersions",
        "lex:listExports",
        "lex:listImports",
        "lex:listIntents",
        "lex:listRecommendedIntents",
        "lex:listSlots",
        "lex:listSlotTypes",
        "license-manager:getLicenseConfiguration",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listResourceInventory",
        "license-manager:listUsageForLicenseConfiguration",
        "lightsail:getActiveNames",
        "lightsail:getAlarms",
```

```
        "lightsail:getAutoSnapshots",
        "lightsail:getBlueprints",
        "lightsail:getBucketBundles",
        "lightsail:getBucketMetricData",
        "lightsail:getBuckets",
        "lightsail:getBundles",
        "lightsail:getCertificates",
        "lightsail:getContainerImages",
        "lightsail:getContainerServiceDeployments",
        "lightsail:getContainerServiceMetricData",
        "lightsail:getContainerServicePowers",
        "lightsail:getContainerServices",
        "lightsail:getDisk",
        "lightsail:getDisks",
        "lightsail:getDiskSnapshot",
        "lightsail:getDiskSnapshots",
        "lightsail:getDistributionBundles",
        "lightsail:getDistributionMetricData",
        "lightsail:getDistributions",
        "lightsail:getDomain",
        "lightsail:getDomains",
        "lightsail:getExportSnapshotRecords",
        "lightsail:getInstance",
        "lightsail:getInstanceMetricData",
        "lightsail:getInstancePortStates",
        "lightsail:getInstances",
        "lightsail:getInstanceSnapshot",
        "lightsail:getInstanceSnapshots",
        "lightsail:getInstanceState",
        "lightsail:getKeyPair",
        "lightsail:getKeyPairs",
        "lightsail:getLoadBalancer",
        "lightsail:getLoadBalancerMetricData",
        "lightsail:getLoadBalancers",
        "lightsail:getLoadBalancerTlsCertificates",
        "lightsail:getOperation",
        "lightsail:getOperations",
        "lightsail:getOperationsForResource",
        "lightsail:getRegions",
        "lightsail:getRelationalDatabase",
        "lightsail:getRelationalDatabaseMetricData",
        "lightsail:getRelationalDatabases",
        "lightsail:getRelationalDatabaseSnapshot",
        "lightsail:getRelationalDatabaseSnapshots",
```

```
        "lightsail:getStaticIp",
        "lightsail:getStaticIps",
        "lightsail:isVpcPeered",
        "logs:describeAccountPolicies",
        "logs:describeDeliveries",
        "logs:describeDeliveryDestinations",
        "logs:describeDeliverySources",
        "logs:describeDestinations",
        "logs:describeExportTasks",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeQueries",
        "logs:describeQueryDefinitions",
        "logs:describeResourcePolicies",
        "logs:describeSubscriptionFilters",
        "logs:getDataProtectionPolicy",
        "logs:getDelivery",
        "logs:getDeliveryDestination",
        "logs:getDeliveryDestinationPolicy",
        "logs:getDeliverySource",
        "logs:getLogAnomalyDetector",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:listAnomalies",
        "logs:listLogAnomalyDetectors",
        "logs:listLogDeliveries",
        "logs:testMetricFilter",
        "lookoutequipment:describeDataIngestionJob",
        "lookoutequipment:describeDataset",
        "lookoutequipment:describeInferenceScheduler",
        "lookoutequipment:describeModel",
        "lookoutequipment:listDataIngestionJobs",
        "lookoutequipment:listDatasets",
        "lookoutequipment:listInferenceExecutions",
        "lookoutequipment:listInferenceSchedulers",
        "lookoutequipment:listModels",
        "lookoutmetrics:describeAlert",
        "lookoutmetrics:describeAnomalyDetectionExecutions",
        "lookoutmetrics:describeAnomalyDetector",
        "lookoutmetrics:describeMetricSet",
        "lookoutmetrics:getAnomalyGroup",
        "lookoutmetrics:getDataQualityMetrics",
        "lookoutmetrics:getFeedback",
```

```
        "lookoutmetrics:getSampleData",
        "lookoutmetrics:listAlerts",
        "lookoutmetrics:listAnomalyDetectors",
        "lookoutmetrics:listAnomalyGroupSummaries",
        "lookoutmetrics:listAnomalyGroupTimeSeries",
        "lookoutmetrics:listMetricSets",
        "lookoutmetrics:listTagsForResource",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:getClassificationExportConfiguration",
        "macie2:getCustomDataIdentifier",
        "macie2:getFindings",
        "macie2:getFindingStatistics",
        "macie2:listClassificationJobs",
        "macie2:listCustomDataIdentifiers",
        "macie2:listFindings",
        "managedblockchain:getMember",
        "managedblockchain:getNetwork",
        "managedblockchain:getNode",
        "managedblockchain:listMembers",
        "managedblockchain:listNetworks",
        "managedblockchain:listNodes",
        "mediaconnect:describeFlow",
        "mediaconnect:listEntitlements",
        "mediaconnect:listFlows",
        "mediaconvert:describeEndpoints",
        "mediaconvert:getJob",
        "mediaconvert:getJobTemplate",
        "mediaconvert:getPreset",
        "mediaconvert:getQueue",
        "mediaconvert:listJobs",
        "mediaconvert:listJobTemplates",
        "medialive:describeChannel",
        "medialive:describeInput",
        "medialive:describeInputDevice",
        "medialive:describeInputSecurityGroup",
        "medialive:describeMultiplex",
        "medialive:describeOffering",
```

```
        "medialive:describeReservation",
        "medialive:describeSchedule",
        "medialive:listChannels",
        "medialive:listInputDevices",
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "mediapackage:describeChannel",
        "mediapackage:describeOriginEndpoint",
        "mediapackage:listChannels",
        "mediapackage:listOriginEndpoints",
        "mediastore:describeContainer",
        "mediastore:getContainerPolicy",
        "mediastore:getCorsPolicy",
        "mediastore:listContainers",
        "mediatailor:getPlaybackConfiguration",
        "mediatailor:listPlaybackConfigurations",
        "medical-imaging:getDatastore",
        "medical-imaging:listDatastores",
        "mgn:describeJobLogItems",
        "mgn:describeJobs",
        "mgn:describeLaunchConfigurationTemplates",
        "mgn:describeReplicationConfigurationTemplates",
        "mgn:describeSourceServers",
        "mgn:describeVcenterClients",
        "mgn:getLaunchConfiguration",
        "mgn:getReplicationConfiguration",
        "mgn:listApplications",
        "mgn:listSourceServerActions",
        "mgn:listTemplateActions",
        "mgn:listWaves",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApp",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
```

```
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getCampaignVersion",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEndpoint",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJob",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJob",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "m2:getApplication",
        "m2:getApplicationVersion",
        "m2:getBatchJobExecution",
        "m2:getDataSetDetails",
        "m2:getDataSetImportTask",
        "m2:getDeployment",
        "m2:getEnvironment",
        "m2:listApplications",
        "m2:listApplicationVersions",
        "m2:listBatchJobDefinitions",
        "m2:listBatchJobExecutions",
        "m2:listDataSetImportHistory",
```

```
        "m2:listDataSets",
        "m2:listDeployments",
        "m2:listEngineVersions",
        "m2:listEnvironments",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeTlsInspectionConfiguration",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listRuleGroups",
        "network-firewall:listTlsInspectionConfigurations",
        "networkmanager:describeGlobalNetworks",
        "networkmanager:getConnectAttachment",
        "networkmanager:getConnections",
        "networkmanager:getConnectPeer",
        "networkmanager:getConnectPeerAssociations",
        "networkmanager:getCoreNetwork",
        "networkmanager:getCoreNetworkChangeEvents",
        "networkmanager:getCoreNetworkChangeSet",
        "networkmanager:getCoreNetworkPolicy",
        "networkmanager:getCustomerGatewayAssociations",
        "networkmanager:getDevices",
        "networkmanager:getLinkAssociations",
        "networkmanager:getLinks",
        "networkmanager:getNetworkResourceCounts",
        "networkmanager:getNetworkResourceRelationships",
        "networkmanager:getNetworkResources",
        "networkmanager:getNetworkRoutes",
        "networkmanager:getNetworkTelemetry",
        "networkmanager:getResourcePolicy",
        "networkmanager:getRouteAnalysis",
        "networkmanager:getSites",
        "networkmanager:getSiteToSiteVpnAttachment",
        "networkmanager:getTransitGatewayConnectPeerAssociations",
        "networkmanager:getTransitGatewayPeering",
        "networkmanager:getTransitGatewayRegistrations",
        "networkmanager:getTransitGatewayRouteTableAttachment",
        "networkmanager:getVpcAttachment",
        "networkmanager:listAttachments",
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
        "networkmanager:listCoreNetworks",
```

```
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "networkmonitor:getMonitor",
        "networkmonitor:getProbe",
        "networkmonitor:listMonitors",
        "nimble:getEula",
        "nimble:getLaunchProfile",
        "nimble:getLaunchProfileDetails",
        "nimble:getLaunchProfileInitialization",
        "nimble:getLaunchProfileMember",
        "nimble:getStreamingImage",
        "nimble:getStreamingSession",
        "nimble:getStreamingSessionStream",
        "nimble:getStudio",
        "nimble:getStudioComponent",
        "nimble:listEulaAcceptances",
        "nimble:listEulas",
        "nimble:listLaunchProfiles",
        "nimble:listStreamingImages",
        "nimble:listStreamingSessions",
        "nimble:listStudioComponents",
        "nimble:listStudios",
        "notifications:getEventRule",
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
        "notifications:listNotificationHubs",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
```

```
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunGroup",
        "omics:getSequenceStore",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferenceStores",
        "omics:listReferences",
        "omics:listRunGroups",
        "omics:listRunTasks",
        "omics:listRuns",
        "omics:listSequenceStores",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
        "omics:listWorkflows",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
        "opsworks:describeRdsDbInstances",
```

```
        "opsworks:describeServiceErrors",
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:listAccounts",
        "organizations:listTagsForResource",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
        "personalize:describeCampaign",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
        "personalize:listDatasetExportJobs",
```

```
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "personalize:listRecipes",
        "personalize:listRecommenders",
        "personalize:listSchemas",
        "personalize:listSolutions",
        "personalize:listSolutionVersions",
        "pipes:describePipe",
        "pipes:listPipes",
        "pipes:listTagsForResource",
        "polly:describeVoices",
        "polly:getLexicon",
        "polly:listLexicons",
        "pricing:describeServices",
        "pricing:getAttributeValues",
        "pricing:getProducts",
        "private-networks:getDeviceIdentifier",
        "private-networks:getNetwork",
        "private-networks:getNetworkResource",
        "private-networks:listDeviceIdentifiers",
        "private-networks:listNetworks",
        "private-networks:listNetworkResources",
        "qbusiness:getApplication",
        "qbusiness:getDataSource",
        "qbusiness:getIndex",
        "qbusiness:getRetriever",
        "qbusiness:getWebExperience",
        "qbusiness:listApplications",
        "qbusiness:listDataSources",
        "qbusiness:listDataSourceSyncJobs",
        "qbusiness:listIndices",
        "qbusiness:listRetrievers",
        "qbusiness:listWebExperiences",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
```

```
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboards",
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
```

```
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEvents",
```

```
        "rds:describeEventSubscriptions",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
```

```
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
        "robomaker:describeFleet",
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
        "robomaker:listRobots",
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
```

```
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
```

```
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
```

```
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
```

```
        "s3:listJobs",
        "s3:listMultipartUploadParts",
        "s3:listMultiRegionAccessPoints",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
```

```
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
```

```
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContents",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImages",
        "sagemaker:listImageVersions",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCards",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
```

```
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "savingsplans:describeSavingsPlans",
        "scheduler:getSchedule",
        "scheduler:getScheduleGroup",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "schemas:describeCodeBinding",
        "schemas:describeDiscoverer",
        "schemas:describeRegistry",
        "schemas:describeSchema",
        "schemas:getCodeBindingSource",
        "schemas:getDiscoveredSchema",
        "schemas:getResourcePolicy",
        "schemas:listDiscoverers",
        "schemas:listRegistries",
        "schemas:listSchemas",
        "schemas:listSchemaVersions",
        "sdb:domainMetadata",
        "sdb:listDomains",
        "secretsmanager:describeSecret",
        "secretsmanager:getResourcePolicy",
        "secretsmanager:listSecrets",
        "secretsmanager:listSecretVersionIds",
        "securityhub:getEnabledStandards",
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:listEnabledProductsForImport",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "securitylake:getDataLakeExceptionSubscription",
        "securitylake:getDataLakeOrganizationConfiguration",
        "securitylake:getDataLakeSources",
```

```
        "securitylake:getSubscriber",
        "securitylake:listDataLakeExceptions",
        "securitylake:listDataLakes",
        "securitylake:listLogSources",
        "securitylake:listSubscribers",
        "serverlessrepo:getApplication",
        "serverlessrepo:getApplicationPolicy",
        "serverlessrepo:getCloudFormationTemplate",
        "serverlessrepo:listApplicationDependencies",
        "serverlessrepo:listApplications",
        "serverlessrepo:listApplicationVersions",
        "servicecatalog:describeConstraint",
        "servicecatalog:describePortfolio",
        "servicecatalog:describeProduct",
        "servicecatalog:describeProductAsAdmin",
        "servicecatalog:describeProductView",
        "servicecatalog:describeProvisioningArtifact",
        "servicecatalog:describeProvisioningParameters",
        "servicecatalog:describeRecord",
        "servicecatalog:listAcceptedPortfolioShares",
        "servicecatalog:listConstraintsForPortfolio",
        "servicecatalog:listLaunchPaths",
        "servicecatalog:listPortfolioAccess",
        "servicecatalog:listPortfolios",
        "servicecatalog:listPortfoliosForProduct",
        "servicecatalog:listPrincipalsForPortfolio",
        "servicecatalog:listProvisioningArtifacts",
        "servicecatalog:listRecordHistory",
        "servicecatalog:scanProvisionedProducts",
        "servicecatalog:searchProducts",
        "servicequotas:getAssociationForServiceQuotaTemplate",
        "servicequotas:getAWSDefaultServiceQuota",
        "servicequotas:getRequestedServiceQuotaChange",
        "servicequotas:getServiceQuota",
        "servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listRequestedServiceQuotaChangeHistory",
        "servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:listServiceQuotas",
        "servicequotas:listServices",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
```

```
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeProtection",
        "shield:describeSubscription",
```

```
        "shield:listAttacks",
        "shield:listProtections",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
        "snowball:describeAddress",
        "snowball:describeAddresses",
        "snowball:describeJob",
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs:listQueues",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
```

```
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotations",
        "ssm-contacts:listRotationShifts",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
        "ssm-sap:getApplication",
        "ssm-sap:getComponent",
        "ssm-sap:getDatabase",
        "ssm-sap:getOperation",
        "ssm-sap:getResourcePermission",
        "ssm-sap:listApplications",
        "ssm-sap:listComponents",
        "ssm-sap:listDatabases",
        "ssm-sap:listOperations",
        "ssm:describeActivations",
        "ssm:describeAssociation",
        "ssm:describeAssociationExecutions",
        "ssm:describeAssociationExecutionTargets",
        "ssm:describeAutomationExecutions",
        "ssm:describeAutomationStepExecutions",
        "ssm:describeAvailablePatches",
        "ssm:describeDocument",
        "ssm:describeDocumentPermission",
        "ssm:describeEffectiveInstanceAssociations",
        "ssm:describeEffectivePatchesForPatchBaseline",
        "ssm:describeInstanceAssociationsStatus",
        "ssm:describeInstanceInformation",
        "ssm:describeInstancePatches",
        "ssm:describeInstancePatchStates",
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutions",
```

```
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroups",
        "ssm:describePatchGroupState",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociations",
        "ssm:listAssociationVersions",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocuments",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocumentVersions",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
```

```
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeApplication",
        "sso:describeInstance",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getManagedApplicationInstance",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
        "states:listStateMachineVersions",
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
```

```
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
        "storagegateway:listFileShares",
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
        "storagegateway:listVolumes",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
```

```
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
        "transcribe:describeLanguageModel",
        "transcribe:getCallAnalyticsCategory",
        "transcribe:getCallAnalyticsJob",
        "transcribe:getMedicalTranscriptionJob",
        "transcribe:getMedicalVocabulary",
        "transcribe:getTranscriptionJob",
        "transcribe:getVocabulary",
        "transcribe:getVocabularyFilter",
        "transcribe:listCallAnalyticsCategories",
        "transcribe:listCallAnalyticsJobs",
        "transcribe:listLanguageModels",
        "transcribe:listMedicalTranscriptionJobs",
        "transcribe:listMedicalVocabularies",
        "transcribe:listTranscriptionJobs",
        "transcribe:listVocabularies",
        "transcribe:listVocabularyFilters",
        "transfer:describeAccess",
        "transfer:describeAgreement",
        "transfer:describeConnector",
        "transfer:describeExecution",
        "transfer:describeProfile",
        "transfer:describeServer",
        "transfer:describeUser",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
        "transfer:listUsers",
        "transfer:listWorkflows",
        "transfer:sendWorkflowStepState",
        "trustedadvisor:getOrganizationRecommendation",
        "trustedadvisor:getRecommendation",
```

```
        "trustedadvisor:listChecks",
        "trustedadvisor:listOrganizationRecommendationAccounts",
        "trustedadvisor:listOrganizationRecommendationResources",
        "trustedadvisor:listOrganizationRecommendations",
        "trustedadvisor:listRecommendationResources",
        "trustedadvisor:listRecommendations",
        "verifiedpermissions:getIdentitySource",
        "verifiedpermissions:getPolicy",
        "verifiedpermissions:getPolicyStore",
        "verifiedpermissions:getPolicyTemplate",
        "verifiedpermissions:getSchema",
        "verifiedpermissions:listIdentitySources",
        "verifiedpermissions:listPolicies",
        "verifiedpermissions:listPolicyStores",
        "verifiedpermissions:listPolicyTemplates",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
```

```
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
```

```
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workdocs:checkAlias",
        "workdocs:describeAvailableDirectories",
        "workdocs:describeInstances",
        "workmail:describeGroup",
        "workmail:describeOrganization",
        "workmail:describeResource",
        "workmail:describeUser",
        "workmail:listAliases",
        "workmail:listGroupMembers",
        "workmail:listGroups",
        "workmail:listMailboxPermissions",
        "workmail:listOrganizations",
        "workmail:listResourceDelegates",
        "workmail:listResources",
        "workmail:listUsers",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
```

```
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus",
        "xray:getEncryptionConfig",
        "xray:getGroup",
        "xray:getGroups",
        "xray:getSamplingRules",
        "xray:listResourcePolicies"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerAccountDiscoveryServicePolicy

Beschreibung: Erteilt AWS Systems Manager (SSM) die Erlaubnis, AWS-Konto Informationen zu ermitteln.

`AWSSystemsManagerAccountDiscoveryServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Oktober 2019, 17:21 Uhr UTC
- Zeit bearbeitet: 17. Oktober 2022, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerChangeManagementServicePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Ressourcen, die vom AWS Systems Manager Change Management Framework verwaltet oder verwendet werden.

`AWSSystemsManagerChangeManagementServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Dezember 2020, 22:21 Uhr UTC
- Bearbeitete Zeit: 7. Dezember 2020, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerForSAPFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Systems Manager for SAP-Service

`AWSSystemsManagerForSAPFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSystemsManagerForSAPFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2022, 02:11 Uhr UTC
- Bearbeitete Zeit: 18. November 2022, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm-sap.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerForSAPReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den AWS Systems Manager for SAP-Service

`AWSSystemsManagerForSAPReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSSystemsManagerForSAPReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 17. November 2022, 02:11 Uhr UTC
- Zeit bearbeitet: 17. November 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Beschreibung: IAM-Rolle für SSM Explorer zur Verwaltung OpsData verwandter Operationen

`AWSSystemsManagerOpsDataSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. April 2021, 20:42 UTC
- Bearbeitete Zeit: 28. Juni 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxAssetServerPolicy

Beschreibung: Diese Richtlinie gewährt dem AWS Portal Asset Server die für den normalen Betrieb erforderlichen Berechtigungen.

`AWSThinkboxAssetServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSThinkboxAssetServerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:18 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxAWSPortalAdminPolicy

Beschreibung: Diese Richtlinie gewährt der Deadline-Software von AWS Thinkbox vollen Zugriff auf mehrere AWS Dienste, die für die AWS Portalverwaltung erforderlich sind. Dies beinhaltet den Zugriff auf die Erstellung beliebiger Tags für verschiedene EC2-Ressourcentypen.

`AWSThinkboxAWSPortalAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSThinkboxAWSPortalAdminPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:41 UTC
- Bearbeitete Zeit: 12. April 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
```

```
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/AWSPortal*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal4",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal5",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
        }
      }
```

```
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:PlacementGroup" : "*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ]
```

```
    },
    {
      "Sid" : "AWSThinkboxAWSPortal10",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal11",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal12",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal13",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
```

```
      "Sid" : "AWSThinkboxAWSPortal14",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal15",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal16",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
```

```
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal17",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-aws-portal-cache*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal18",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
      ]
```

```
    },
    {
      "Sid" : "AWSThinkboxAWSPortal19",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal20",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal21",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",
        "arn:aws:cloudformation:*:*:stack/Deadline*/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal22",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:EstimateTemplateCost",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal23",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal24",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal25",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AWSThinkboxAWSPortal26",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : [
            "rcs-tls-pw*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal27",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxAWSPortalGatewayPolicy

Beschreibung: Diese Richtlinie gewährt dem AWS Portal Gateway-Computer die für den normalen Betrieb erforderlichen Berechtigungen.

`AWSThinkboxAWSPortalGatewayPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSThinkboxAWSPortalGatewayPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:05 UTC
- Bearbeitete Zeit: 30. Juni 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxAWSPortalWorkerPolicy

Beschreibung: Diese Richtlinie gewährt den Deadline Workers im AWS Portal die erforderlichen Berechtigungen, die für den normalen Betrieb erforderlich sind.

`AWSThinkboxAWSPortalWorkerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSThinkboxAWSPortalWorkerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:15 UTC
- Bearbeitete Zeit: 7. Dezember 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Beschreibung: Erteilt die für den Betrieb des Deadline Resource Trackers von AWS Thinkbox erforderlichen Berechtigungen. Dies beinhaltet den vollen Zugriff auf einige EC2-Aktionen, einschließlich DeleteFleets und. CancelSpotFleetRequests

`AWSThinkboxDeadlineResourceTrackerAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSThinkboxDeadlineResourceTrackerAccessPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:25 UTC

- Bearbeitete Zeit: 27. Mai 2020, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Beschreibung: Erteilt die erforderlichen Berechtigungen, um den Deadline Resource Tracker von AWS Thinkbox zu erstellen, zu löschen und zu verwalten.

`AWSThinkboxDeadlineResourceTrackerAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSThinkboxDeadlineResourceTrackerAdminPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:29 UTC
- Bearbeitete Zeit: 12. April 2024, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker1",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker3",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker4",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListTagsOfResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker5",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker6",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
      ]
```

```
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker7",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker8",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker9",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker12",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker13",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker14",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker15",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
```

```
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker16",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker-*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate-*.yaml"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker17",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Beschreibung: Erteilt die für das Deadline Spot Event Plugin von AWS Thinkbox erforderlichen Berechtigungen. Dazu gehören die Erlaubnis, eine Spot-Flotte anzufordern, zu ändern und zu stornieren, sowie eingeschränkte PassRole Genehmigungen.

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSThinkboxDeadlineSpotEventPluginAdminPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:38 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Beschreibung: Erteilen Sie die erforderlichen Berechtigungen für eine EC2-Instance, auf der die AWS Thinkbox Deadline Spot Event Plugin Worker-Software ausgeführt wird.

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:35 UTC
- Bearbeitete Zeit: 7. Dezember 2020, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransferConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Transfer über AWS Management Console

`AWSTransferConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSTransferConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Dezember 2020, 19:33 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransferFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Transfer-Service.

`AWSTransferFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSTransferFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Dezember 2020, 19:37 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransferLoggingAccess

Beschreibung: Ermöglicht AWS Transfer vollen Zugriff, um Protokollstreams und -gruppen zu erstellen und Protokollereignisse in Ihrem Konto zu speichern

`AWSTransferLoggingAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSTransferLoggingAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Januar 2019, 15:32 Uhr UTC
- Bearbeitete Zeit: 14. Januar 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransferReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf die AWS Transferdienste.

`AWSTransferReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSTransferReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. August 2020, 17:54 Uhr UTC
- Bearbeitete Zeit: 27. August 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTrustedAdvisorPriorityFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Trusted Advisor Priority. Diese Richtlinie ermöglicht es dem Benutzer auch, Trusted Advisor als vertrauenswürdigen Dienst bei AWS Organizations hinzuzufügen und delegierte Administratorkonten für Trusted Advisor Priority anzugeben.

`AWSTrustedAdvisorPriorityFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSTrustedAdvisorPriorityFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. August 2022, 16:08 UTC
- Bearbeitete Zeit: 16. August 2022, 16:08 UTC

- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTrustedAdvisorPriorityReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Trusted Advisor Priority. Dies beinhaltet die Berechtigung, die delegierten Administratorkonten einzusehen.

`AWSTrustedAdvisorPriorityReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSTrustedAdvisorPriorityReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. August 2022, 16:35 UTC
- Bearbeitete Zeit: 16. August 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTrustedAdvisorReportingServiceRolePolicy

Beschreibung: Servicerichtlinie für Trusted Advisor Multi-Account-Reporting

`AWSTrustedAdvisorReportingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. November 2019, 17:41 Uhr UTC
- Bearbeitete Zeit: 28. Februar 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTrustedAdvisorServiceRolePolicy

Beschreibung: Zugriff auf den AWS Trusted Advisor Service, um Kosten zu senken, die Leistung zu steigern und die Sicherheit Ihrer AWS Umgebung zu verbessern.

`AWSTrustedAdvisorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. Februar 2018, 21:24 Uhr UTC
- Bearbeitete Zeit: 11. Juni 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "dax:DescribeClusters",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:GetManagedPrefixListEntries",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GenerateCredentialReport",
```

```
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "iam:ListSAMLProviders",
        "kinesis:DescribeLimits",
        "kafka:DescribeClusterV2",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "network-firewall:ListFirewalls",
        "network-firewall:DescribeFirewall",
        "outposts:ListAssets",
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
```

```
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSUserNotificationsServiceLinkedRolePolicy

Beschreibung: Ermöglicht AWS Benutzerbenachrichtigungen, AWS Dienste in Ihrem Namen aufzurufen.

`AWSUserNotificationsServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. April 2023, 13:28 UTC
- Bearbeitete Zeit: 19. April 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVendorInsightsAssessorFullAccess

Beschreibung: Bietet vollen Zugriff zum Anzeigen berechtigter Vendor Insights-Ressourcen und zum Verwalten von Vendor Insights-Abonnements

`AWSVendorInsightsAssessorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSVendorInsightsAssessorFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVendorInsightsAssessorReadOnly

Beschreibung: Bietet Lesezugriff zum Anzeigen berechtigter Ressourcen von Vendor Insights

`AWSVendorInsightsAssessorReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSVendorInsightsAssessorReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVendorInsightsVendorFullAccess

Beschreibung: Bietet vollen Zugriff auf die Erstellung und Verwaltung der Vendor Insights-Ressourcen

`AWSVendorInsightsVendorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSVendorInsightsVendorFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 19. Oktober 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVendorInsightsVendorReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff zum Anzeigen der Vendor Insights-Ressourcen

`AWSVendorInsightsVendorReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSVendorInsightsVendorReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 00:54 UTC

- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVpcLatticeServiceRolePolicy

Beschreibung: Ermöglicht VPC Lattice, in Ihrem Namen auf AWS Ressourcen zuzugreifen.

`AWSVpcLatticeServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2022, 20:47 UTC
- Bearbeitete Zeit: 30. November 2022, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVPCS2SVpnServiceRolePolicy

Beschreibung: Erlauben Sie Site-to-Site VPN, Ressourcen im Zusammenhang mit Ihren VPN-Verbindungen zu erstellen und zu verwalten.

`AWSVPCS2SVpnServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. August 2019, 14:13 Uhr UTC
- Bearbeitete Zeit: 6. August 2019, 14:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVPCTransitGatewayServiceRolePolicy

Beschreibung: Erlauben Sie VPC Transit Gateway, die erforderlichen Ressourcen für Ihre Transit Gateway Gateway-VPC-Anhänge zu erstellen und zu verwalten.

`AWSVPCTransitGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 16:21 UTC
- Bearbeitete Zeit: 15. April 2021, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVPCVerifiedAccessServiceRolePolicy

Beschreibung: Richtlinie zur Aktivierung des AWS Verified Access-Dienstes zur Bereitstellung von Endpunkten in Ihrem Namen

`AWSVPCVerifiedAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2022, 03:35 UTC
- Bearbeitete Zeit: 17. November 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWAFConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS WAF über die AWS Management Console. Beachten Sie, dass diese Richtlinie auch Berechtigungen zum Auflisten und Aktualisieren von CloudFront Amazon-Distributionen, Berechtigungen zum Anzeigen von Load Balancern auf AWS Elastic Load Balancing, Berechtigungen zum Anzeigen von Amazon API Gateway-REST-APIs und -Stages, Berechtigungen zum Auflisten und Anzeigen von CloudWatch Amazon-Metriken sowie Berechtigungen zum Anzeigen von Regionen gewährt, die innerhalb des Kontos aktiviert sind.

`AWSWAFConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSWAFConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. April 2020, 18:38 UTC
- Bearbeitete Zeit: 5. Juni 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:SetWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:UpdateDistribution",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:SetWebACL",
        "appsync:ListGraphqlApis",
        "appsync:SetWebACL",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "s3:ListAllMyBuckets",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "cognito-idp:ListUserPools",
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:AssociateWebAcl",
```

```
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWAFConsoleReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS WAF über die. AWS Management Console Beachten Sie, dass diese Richtlinie auch Berechtigungen zum Auflisten von CloudFront Amazon-Distributionen, Berechtigungen zum Anzeigen von Load Balancern auf AWS Elastic Load Balancing, Berechtigungen zum Anzeigen von Amazon API Gateway-REST-APIs und -Stages, Berechtigungen zum Auflisten und Anzeigen von CloudWatch Amazon-Metriken sowie Berechtigungen zum Anzeigen von Regionen gewährt, die innerhalb des Kontos aktiviert sind.

`AWSWAFConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSWAFConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. April 2020, 18:43 UTC
- Bearbeitete Zeit: 5. Juni 2023, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "apigateway:GET",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "appsync:ListGraphqlApis",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:CheckCapacity",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstances"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWAFFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS WAF-Aktionen.

`AWSWAFFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSWAFFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Oktober 2015, 20:44 UTC
- Bearbeitete Zeit: 5. Juni 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*",
        "wafv2:*",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "appsync:SetWebACL",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWAFReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS WAF-Aktionen.

`AWSWAFReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSWAFReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Oktober 2015, 20:43 UTC
- Bearbeitete Zeit: 5. Juni 2023, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
```

```
        "waf-regional:List*",
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity",
        "cognito-idp:ListResourcesForWebACL",
        "cognito-idp:GetWebACLForResource",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWellArchitectedDiscoveryServiceRolePolicy

Beschreibung: Ermöglicht WellArchitected den Zugriff auf AWS Dienste und Ressourcen, die sich auf WellArchitected Ressourcen im Namen von Kunden beziehen.

`AWSWellArchitectedDiscoveryServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. April 2023, 18:36 UTC
- Bearbeitete Zeit: 26. April 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWellArchitectedOrganizationsServiceRolePolicy

Beschreibung: Ermöglicht Well-Architected, in Ihrem Namen auf Organizations zuzugreifen.

`AWSWellArchitectedOrganizationsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. Juni 2022, 17:15 UTC
- Bearbeitete Zeit: 25. Juli 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWickrFullAccess

Beschreibung: Diese Richtlinie gewährt dem Wickr-Dienst vollständige Administratorrechte, einschließlich der Wickr-Verwaltungsfunktionen unter. AWS Management Console

`AWSWickrFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSWickrFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 20:36 UTC

- Zeit bearbeitet: 27. November 2022, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXrayCrossAccountSharingConfiguration

Beschreibung: Bietet Funktionen zur Verwaltung von Observability Access Manager-Links und zur gemeinsamen Nutzung von X-Ray-Traces

`AWSXrayCrossAccountSharingConfiguration`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSXrayCrossAccountSharingConfiguration` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 13:46 UTC
- Zeit bearbeitet: 27. November 2022, 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXRayDaemonWriteAccess

Beschreibung: Erlaubt dem AWS X-Ray-Daemon, rohe Trace-Segmentdaten an die API des Dienstes weiterzuleiten und Sampling-Daten (Regeln, Ziele usw.) abzurufen, die vom X-Ray-SDK verwendet werden können.

`AWSXRayDaemonWriteAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSXRayDaemonWriteAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. August 2018, 23:00 Uhr UTC
- Bearbeitete Zeit: 13. Februar 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXrayFullAccess

Beschreibung: Verwaltete AWS X-Ray-Richtlinie mit vollem Zugriff

`AWSXrayFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSXrayFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 18:30 Uhr UTC
- Bearbeitete Zeit: 11. April 2024, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXrayReadOnlyAccess

Beschreibung: Verwaltete AWS X-Ray-Richtlinie nur zum Lesen

`AWSXrayReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSXrayReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 18:27 UTC
- Bearbeitete Zeit: 14. Februar 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXrayWriteOnlyAccess

Beschreibung: Verwaltete AWS X-Ray-Richtlinie nur zum Schreiben

`AWSXrayWriteOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `AWSXrayWriteOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 18:19 Uhr UTC
- Bearbeitete Zeit: 28. August 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSZonalAutoshiftPracticeRunSLRPolicy

Beschreibung: Bietet administrativen Zugriff auf Übungsläufe in ARC-Zonenschichten sowie Zugriff auf CloudWatch Alarmstatus zur Überwachung von Übungsläufen.

`AWSZonalAutoshiftPracticeRunSLRPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2023, 17:34 UTC
- Bearbeitete Zeit: 29. November 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

BatchServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf den AWS Batch-Service zur Verwaltung der erforderlichen Ressourcen, einschließlich Amazon EC2- und Amazon ECS-Ressourcen.

`BatchServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. März 2021, 06:55 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Billing

Beschreibung: Erteilt Berechtigungen für die Abrechnung und das Kostenmanagement. Dazu gehören das Anzeigen der Kontonutzung sowie das Anzeigen und Ändern von Budgets und Zahlungsmethoden.

`Billing`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `Billing` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Art: Richtlinie für Job Funktionen

- Erstellungszeit: 10. November 2016, 17:33 Uhr UTC
- Bearbeitete Zeit: 23. Mai 2024, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:UpdateBillingPreferences",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
```

```
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
        "budgets:UpdateBudgetAction",
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce:DeleteCostCategoryDefinition",
        "ce:DeleteNotificationSubscription",
        "ce:DeleteReport",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:TagResource",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:UpdateNotificationSubscription",
        "ce:UpdatePreferences",
        "ce:UpdateReport",
        "ce:UpdateCostCategoryDefinition",
        "ce:UntagResource",
        "ce:StartCostAllocationTagBackfill",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:ModifyReportDefinition",
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
```

```
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "payments:ListTagsForResource",
        "payments:ListPaymentInstruments",
        "payments:MakePayment",
        "payments:TagResource",
        "payments:UpdatePaymentPreferences",
        "payments:UpdatePaymentInstrument",
        "payments:UntagResource",
        "pricing:DescribeServices",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "support:CreateCase",
        "support:AddAttachmentsToSet",
        "sustainability:GetCarbonFootprintSummary",
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
        "tax:UpdateExemptions"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CertificateManagerServiceRolePolicy

Beschreibung: Amazon Certificate Manager Service Rollenrichtlinie

`CertificateManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Juni 2020, 17:56 Uhr UTC
- Bearbeitete Zeit: 25. Juni 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ClientVPNServiceConnectionsRolePolicy

Beschreibung: Richtlinie, mit der AWS Client VPN Ihre Client-VPN-Endpunktverbindungen verwalten kann.

`ClientVPNServiceConnectionsRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. August 2020, 19:48 UTC
- Bearbeitete Zeit: 12. August 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ClientVPNServiceRolePolicy

Beschreibung: Richtlinie zur Aktivierung von AWS Client VPN zur Verwaltung Ihrer Client-VPN-Endpunkte.

`ClientVPNServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Dezember 2018, 21:20 Uhr UTC
- Bearbeitete Zeit: 12. August 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudFormationStackSetsOrgAdminServiceRolePolicy

Beschreibung: Servicerolle für CloudFormation StackSets (Unternehmens-Hauptkonto)

`CloudFormationStackSetsOrgAdminServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Dezember 2019, 00:20 Uhr UTC
- Bearbeitete Zeit: 10. Dezember 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudFormationStackSetsOrgMemberServiceRolePolicy

Beschreibung: Servicerolle für CloudFormation StackSets (Mitgliedskonto der Organisation)

`CloudFormationStackSetsOrgMemberServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. Dezember 2019, 23:52 Uhr UTC
- Bearbeitete Zeit: 9. Dezember 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudFrontFullAccess

Beschreibung: Bietet vollen Zugriff auf die CloudFront Konsole sowie die Möglichkeit, Amazon S3 S3-Buckets über die AWS Management Console aufzulisten.

`CloudFrontFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudFrontFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 4. Januar 2024, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Action" : [
```

```
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "kinesis:ListStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "cffdescribestream",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Action" : [
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudFrontReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf Informationen zur CloudFront Distributionskonfiguration und Listenverteilungen über die AWS Management Console.

`CloudFrontReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudFrontReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 4. Januar 2024, 16:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudHSMServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Ressourcen, die von CloudHSM verwendet oder verwaltet werden

`CloudHSMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. November 2017, 19:12 UTC
- Zeit bearbeitet: 6. November 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudSearchFullAccess

Beschreibung: Bietet vollen Zugriff auf den CloudSearch Amazon-Konfigurationsservice.

`CloudSearchFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudSearchFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudSearchReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den CloudSearch Amazon-Konfigurationsservice.

`CloudSearchReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudSearchReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudTrailServiceRolePolicy

Beschreibung: Berechtigungsrichtlinie für CloudTrail ServiceLinkedRole

`CloudTrailServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Oktober 2018, 21:21 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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}"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatch-CrossAccountAccess

Beschreibung: Ermöglicht CloudWatch die Übernahme von CrossAccountSharing Rollen in Remote-Konten im Namen des aktuellen Kontos, um Daten konto CloudWatch - und regionsübergreifend anzuzeigen

`CloudWatch-CrossAccountAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. Juli 2019, 09:59 Uhr UTC
- Bearbeitete Zeit: 23. Juli 2019, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchActionsEC2Access

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch Alarme und Metriken sowie auf EC2-Metadaten. Ermöglicht den Zugriff auf EC2-Instances zum Stoppen, Beenden und Neustarten.

`CloudWatchActionsEC2Access`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchActionsEC2Access` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Juli 2015, 00:00 Uhr UTC
- Bearbeitete Zeit: 7. Juli 2015, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchAgentAdminPolicy

Beschreibung: Für die Verwendung sind vollständige Berechtigungen erforderlich AmazonCloudWatchAgent.

`CloudWatchAgentAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchAgentAdminPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. März 2018, 00:52 UTC
- Zeit bearbeitet: 5. Februar 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchAgentServerPolicy

Beschreibung: Für die Verwendung AmazonCloudWatchAgent auf Servern sind Berechtigungen erforderlich

`CloudWatchAgentServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchAgentServerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. März 2018, 01:06 UTC
- Bearbeitete Zeit: 6. Februar 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationInsightsFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch Application Insights und die erforderlichen Abhängigkeiten.

`CloudWatchApplicationInsightsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchApplicationInsightsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. November 2020, 18:44 Uhr UTC
- Bearbeitete Zeit: 25. Januar 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationInsightsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch Application Insights.

`CloudWatchApplicationInsightsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchApplicationInsightsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. November 2020, 18:48 Uhr UTC
- Bearbeitete Zeit: 24. November 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Beschreibung: Richtlinie für verknüpfte Rollen mit dem Cloudwatch Application Insights Service

`CloudwatchApplicationInsightsServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Dezember 2018, 16:22 UTC
- Bearbeitete Zeit: 11. Mai 2023, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v24 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:CreateStack",
        "cloudFormation:UpdateStack",
        "cloudFormation:DeleteStack",
        "cloudFormation:DescribeStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:DescribeStacks",
        "cloudFormation:ListStackResources",
        "cloudFormation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
```

```
        "ssm:RemoveTagsFromResource",
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:CreateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:UpdateOpsItem",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-CheckPerformanceCounterSets",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:document/AWSEC2-DetectWorkload",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetTraceGraph"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateClusterSettings"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:GetSMSAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationSignalsFullAccess

Beschreibung: Bieten Sie vollen Zugriff auf den CloudWatch Application Signals-Dienst und bereichsspezifischen Zugriff auf die Abhängigkeiten, die für die Nutzung und den Betrieb dieses Dienstes erforderlich sind.

`CloudWatchApplicationSignalsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchApplicationSignalsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. Juni 2024, 22:50 UTC
- Bearbeitungszeit: 6. Juni 2024, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : "application-signals:*",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudWatchApplicationSignalsRumPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchCreateRumMetricDefinitions",
        "rum:BatchDeleteRumMetricDefinitions",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:PutRumMetricsDestination",
        "rum:UpdateRumMetricDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
      "Effect" : "Allow",
      "Action" : "xray:GetTraceSummaries",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
```

```
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:cloudwatch-application-signals-*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
      "Effect" : "Allow",
      "Action" : "sns:ListTopics",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationSignalsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den CloudWatch Application Signals-Dienst und bereichsspezifischen Zugriff auf die Abhängigkeiten, die für die Nutzung dieses Dienstes erforderlich sind

`CloudWatchApplicationSignalsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchApplicationSignalsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. Juni 2024, 22:48 UTC
- Bearbeitungszeit: 6. Juni 2024, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationSignalsServiceRolePolicy

Beschreibung: Die Richtlinie erteilt CloudWatch Application Signals die Erlaubnis, Überwachungs- und Kennzeichnungsdaten von anderen relevanten AWS Diensten zu sammeln.

`CloudWatchApplicationSignalsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. November 2023, 18:09 UTC
- Bearbeitete Zeit: 26. April 2024, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "xray:GetServiceGraph"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWListMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "CWGetMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2AutoScalingPermission",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchAutomaticDashboardsAccess

Beschreibung: Bietet Zugriff auf CloudWatch Nicht-APIs, die zur Anzeige von CloudWatch automatischen Dashboards verwendet werden, einschließlich des Inhalts von Objekten wie Lambda-Funktionen

`CloudWatchAutomaticDashboardsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchAutomaticDashboardsAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Juli 2019, 10:01 UTC
- Bearbeitete Zeit: 20. April 2021, 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchCrossAccountSharingConfiguration

Beschreibung: Bietet Funktionen zur Verwaltung von Observability Access Manager-Links und zur Einrichtung der gemeinsamen Nutzung von CloudWatch Ressourcen

`CloudWatchCrossAccountSharingConfiguration`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchCrossAccountSharingConfiguration` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 14:01 UTC
- Bearbeitete Zeit: 27. November 2022, 14:01 UTC

- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsBuiltInTargetExecutionAccess

Beschreibung: Ermöglicht integrierten Zielen in Amazon CloudWatch Events, EC2-Aktionen in Ihrem Namen durchzuführen.

`CloudWatchEventsBuiltInTargetExecutionAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchEventsBuiltInTargetExecutionAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Januar 2016, 18:35 Uhr UTC
- Bearbeitete Zeit: 14. Januar 2016, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon CloudWatch Events.

`CloudWatchEventsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchEventsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Januar 2016, 18:37 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
AmazonEventBridgeApiDestinationsServiceRolePolicy",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleForCloudWatchEvents",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS_Events_Invoke_Targets"
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsInvocationAccess

Beschreibung: Ermöglicht Amazon CloudWatch Events, Ereignisse an die Streams in AWS Kinesis Streams in Ihrem Konto weiterzuleiten.

`CloudWatchEventsInvocationAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchEventsInvocationAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Januar 2016, 18:36 Uhr UTC
- Bearbeitete Zeit: 14. Januar 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon CloudWatch Events.

`CloudWatchEventsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchEventsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Januar 2016, 18:27 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsServiceRolePolicy

Beschreibung: Ermöglicht AWS CloudWatch die Ausführung von Aktionen in Ihrem Namen, die über Alarme und Ereignisse konfiguriert wurden.

`CloudWatchEventsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. November 2017, 00:42 UTC
- Zeit bearbeitet: 17. November 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch.

`CloudWatchFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 27. November 2022, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchFullAccessV2

Beschreibung: Bietet vollen Zugriff auf CloudWatch.

`CloudWatchFullAccessV2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchFullAccessV2` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. August 2023, 11:32 UTC
- Bearbeitete Zeit: 17. Mai 2024, 22:20 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:*",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
```

```
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchInternetMonitorServiceRolePolicy

Beschreibung: Ermöglicht Internet Monitor, in Ihrem Namen auf EC2, Workspaces und CloudFront Ressourcen sowie andere erforderliche Dienste zuzugreifen.

`CloudWatchInternetMonitorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. November 2022, 17:46 UTC
- Bearbeitete Zeit: 20. Juli 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLambdaInsightsExecutionRolePolicy

Beschreibung: Für die Lambda Insights-Erweiterung ist eine Richtlinie erforderlich

`CloudWatchLambdaInsightsExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchLambdaInsightsExecutionRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2020, 19:27 UTC
- Zeit bearbeitet: 7. Oktober 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLogsCrossAccountSharingConfiguration

Beschreibung: Bietet Funktionen zur Verwaltung von Observability Access Manager-Links und zur gemeinsamen Nutzung von CloudWatch Logs-Ressourcen

`CloudWatchLogsCrossAccountSharingConfiguration`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchLogsCrossAccountSharingConfiguration` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 13:55 UTC
- Zeit bearbeitet: 27. November 2022, 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLogsFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch Protokolle

`CloudWatchLogsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchLogsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLogsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch Protokolle

`CloudWatchLogsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchLogsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
```

```
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchNetworkMonitorServiceRolePolicy

Beschreibung: Ermöglicht CloudWatch Network Monitor den Zugriff auf und die Verwaltung von EC2- und VPC-Ressourcen, die Veröffentlichung von Daten CloudWatch und den Zugriff auf andere erforderliche Dienste in Ihrem Namen.

`CloudWatchNetworkMonitorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Dezember 2023, 18:53 UTC

- Bearbeitete Zeit: 21. Dezember 2023, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
    {
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch.

`CloudWatchReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 17. Mai 2024, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
```

```
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchReadOnlyGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchSyntheticsFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch Synthetics.

`CloudWatchSyntheticsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchSyntheticsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. November 2019, 17:39 Uhr UTC
- Bearbeitete Zeit: 6. Mai 2022, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces",
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::cw-syn-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "synthetics.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:GetFunctionConfiguration",
        "lambda:DeleteFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:cwsyn-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion",
        "lambda:PublishLayerVersion",
        "lambda:DeleteLayerVersion"
      ],
```

```
      "Resource" : [
        "arn:aws:lambda:*:*:layer:cwsyn-*",
        "arn:aws:lambda:*:*:layer:Synthetics:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchSyntheticsReadOnlyAccess

Beschreibung: Bietet Nur-Lese-Zugriff auf CloudWatch Synthetics.

`CloudWatchSyntheticsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CloudWatchSyntheticsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. November 2019, 17:45 Uhr UTC
- Bearbeitete Zeit: 6. März 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComprehendDataAccessRolePolicy

Beschreibung: Richtlinie für die AWS Servicerolle Comprehend, die den Zugriff auf S3-Ressourcen für den Datenzugriff ermöglicht

`ComprehendDataAccessRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ComprehendDataAccessRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 06. März 2019, 22:28 UTC
- Bearbeitete Zeit: 6. März 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComprehendFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Comprehend.

`ComprehendFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ComprehendFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 18:08 Uhr UTC
- Bearbeitete Zeit: 5. Dezember 2017, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComprehendMedicalFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Comprehend Medical

`ComprehendMedicalFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ComprehendMedicalFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 17:55 Uhr UTC
- Bearbeitete Zeit: 27. November 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComprehendReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Comprehend.

`ComprehendReadOnly`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `ComprehendReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 18:10 Uhr UTC
- Bearbeitete Zeit: 26. April 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComputeOptimizerReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf ComputeOptimizer.

`ComputeOptimizerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ComputeOptimizerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. März 2020, 00:11 UTC
- Bearbeitete Zeit: 28. August 2023, 19:22 UTC

- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
```

```
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComputeOptimizerServiceRolePolicy

Beschreibung: Ermöglicht ComputeOptimizer das Aufrufen von AWS Diensten und das Sammeln von Workload-Details in Ihrem Namen.

`ComputeOptimizerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Dezember 2019, 08:45 Uhr UTC
- Bearbeitete Zeit: 13. Juni 2022, 19:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ConfigConformsServiceRolePolicy

Beschreibung: Richtlinie, die für AWSConfig die Erstellung von Konformitätspaketen erforderlich ist

`ConfigConformsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Juli 2019, 21:38 Uhr UTC
- Bearbeitete Zeit: 12. Januar 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CostOptimizationHubAdminAccess

Beschreibung: Diese verwaltete Richtlinie bietet Administratorzugriff auf Cost Optimization Hub.

`CostOptimizationHubAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CostOptimizationHubAdminAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Dezember 2023, 00:03 Uhr UTC
- Bearbeitete Zeit: 19. Dezember 2023, 00:03 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CostOptimizationHubReadOnlyAccess

Beschreibung: Diese verwaltete Richtlinie bietet schreibgeschützten Zugriff auf Cost Optimization Hub.

`CostOptimizationHubReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `CostOptimizationHubReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Dezember 2023, 18:04 UTC
- Bearbeitete Zeit: 13. Dezember 2023, 18:04 UTC

- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CostOptimizationHubServiceRolePolicy

Beschreibung: Ermöglicht Cost Optimization Hub, Unternehmensinformationen abzurufen und optimierungsbezogene Daten und Metadaten zu sammeln.

`CostOptimizationHubServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2023, 08:03 UTC
- Bearbeitete Zeit: 26. November 2023, 08:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CustomerProfilesServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Connect Connect-Kundenprofilen den Zugriff auf AWS Dienste und Ressourcen in Ihrem Namen.

`CustomerProfilesServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. März 2023, 22:56 UTC
- Bearbeitete Zeit: 7. März 2023, 22:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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_*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DatabaseAdministrator

Beschreibung: Gewährt volle Zugriffsberechtigungen für AWS Dienste und Aktionen, die für die Einrichtung und Konfiguration von AWS Datenbankdiensten erforderlich sind.

`DatabaseAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `DatabaseAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:25 Uhr UTC
- Bearbeitete Zeit: 8. Januar 2019, 00:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticache:*",
        "iam:ListRoles",
        "iam:GetRole",
        "kms:ListKeys",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteFunction",
```

```
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:Create*",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "rds:*",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Get*",
        "sns:List*",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutLifecycleConfiguration",
        "s3:PutReplicationConfiguration",
        "s3:PutObject*",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/rdbms-lambda-access",
        "arn:aws:iam::*:role/lambda_exec_role",
        "arn:aws:iam::*:role/lambda-dynamodb-*",
        "arn:aws:iam::*:role/lambda-vpc-execution-role",
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DataScientist

Beschreibung: Erteilt Berechtigungen für AWS Datenanalysedienste.

`DataScientistist` eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `DataScientist` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:28 Uhr UTC

- Bearbeitete Zeit: 3. Dezember 2019, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DAXServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht es DAX, Netzwerkschnittstelle, Sicherheitsgruppe, Subnetz und VPC im Namen des Kunden zu erstellen und zu verwalten

`DAXServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. März 2018, 17:51 UTC
- Bearbeitete Zeit: 5. März 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Beschreibung: Für die Unterstützung von Amazon CloudWatch Contributor Insights for Amazon DynamoDB sind Berechtigungen erforderlich.

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2019, 21:13 Uhr UTC
- Bearbeitete Zeit: 15. November 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DynamoDBKinesisReplicationServiceRolePolicy

Beschreibung: Bieten Sie AWS DynamoDB-Zugriff auf KinesisDataStreams

`DynamoDBKinesisReplicationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. November 2020, 00:43 UTC
- Zeit bearbeitet: 12. November 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DynamoDBReplicationServiceRolePolicy

Beschreibung: Von DynamoDB für die regionsübergreifende Datenreplikation benötigte Berechtigungen

`DynamoDBReplicationServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. November 2017, 23:55 UTC
- Bearbeitete Zeit: 8. Januar 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2FastLaunchFullAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf EC2 Fast Launch-Aktionen

`EC2FastLaunchFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `EC2FastLaunchFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Mai 2024, 22:45 UTC
- Bearbeitete Zeit: 13. Mai 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/EC2FastLaunchFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2FastLaunch",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:EnableFastLaunch",
        "ec2:DisableFastLaunch",
        "ec2:DescribeFastLaunchImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2LaunchInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Sid" : "EC2LaunchInstanceWithVolAndInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "EC2Tags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "IAMSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2fastlaunch.amazonaws.com/
AWSServiceRoleForEC2FastLaunch",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLRPassRole",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2FastLaunchServiceRolePolicy

Beschreibung: Die Richtlinie gewährt ec2fastlaunch die Möglichkeit, vorab bereitgestellte Snapshots im Kundenkonto vorzubereiten und zu verwalten und zugehörige Metriken zu veröffentlichen.

`EC2FastLaunchServiceRolePolicy`ist eine verwaltete AWS Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Januar 2022, 13:08 UTC
- Bearbeitete Zeit: 10. Januar 2022, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTaggedSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "StringLike" : {
          "aws:RequestTag/CreatedByLaunchTemplateVersion" : "*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedByLaunchTemplateName",
            "CreatedByLaunchTemplateId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EC2"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2FleetTimeShiftableServiceRolePolicy

Beschreibung: Richtlinie, die der EC2-Flotte die Erlaubnis erteilt, Instances in future zu starten.

`EC2FleetTimeShiftableServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. Dezember 2019, 19:47 UTC
- Bearbeitete Zeit: 23. Dezember 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Ec2ImageBuilderCrossAccountDistributionAccess

Beschreibung: EC2 Image Builder benötigt Berechtigungen, um eine kontenübergreifende Verteilung durchzuführen.

`Ec2ImageBuilderCrossAccountDistributionAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `Ec2ImageBuilderCrossAccountDistributionAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2020, 19:22 UTC
- Bearbeitete Zeit: 30. September 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2ImageBuilderLifecycleExecutionPolicy

Beschreibung: Die ImageBuilderLifecycleExecutionPolicy EC2-Richtlinie gewährt Image Builder die Erlaubnis, Aktionen wie das Verwerfen oder Löschen von Image Builder Builder-Image-Ressourcen und den ihnen zugrunde liegenden Ressourcen (AMIs, Snapshots) auszuführen, um automatisierte Regeln für Image-Lebenszyklusverwaltungsaufgaben zu unterstützen.

`EC2ImageBuilderLifecycleExecutionPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `EC2ImageBuilderLifecycleExecutionPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 16. November 2023, 23:23 UTC
- Bearbeitete Zeit: 16. November 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2InstanceConnect

Beschreibung: Ermöglicht Kunden, EC2 Instance Connect aufzurufen, um kurzlebige Schlüssel für ihre EC2-Instances zu veröffentlichen und Connect über SSH oder die EC2 Instance Connect-CLI herzustellen.

`EC2InstanceConnect`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `EC2InstanceConnect` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2019, 18:53 Uhr UTC
- Bearbeitete Zeit: 27. Juni 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Ec2InstanceConnectEndpoint

Beschreibung: EC2 Instance Connect-Endpunktrichtlinie zur Verwaltung von vom Kunden erstellten EC2 Instance Connect-Endpunkten

`Ec2InstanceConnectEndpoint`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Januar 2023, 20:19 UTC
- Bearbeitete Zeit: 24. Januar 2023, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "Null" : {
          "aws:RequestTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "Null" : {
          "aws:RequestTag/InstanceConnectEndpointId" : "false"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2InstanceProfileForImageBuilder

Beschreibung: EC2-Instanzprofil für den Image Builder Builder-Dienst.

`EC2InstanceProfileForImageBuilder`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `EC2InstanceProfileForImageBuilder` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2019, 19:08 UTC
- Bearbeitete Zeit: 27. August 2020, 16:40 UTC

- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
```

```
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2InstanceProfileForImageBuilderECRContainerBuilds

Beschreibung: EC2-Instanzprofil zum Erstellen von Container-Images mit EC2 Image Builder. Diese Richtlinie gewährt dem Benutzer umfassende Rechte zum Hochladen von ECR-Bildern.

`EC2InstanceProfileForImageBuilderECRContainerBuilds`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `EC2InstanceProfileForImageBuilderECRContainerBuilds` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 11. Dezember 2020, 19:48 UTC
- Bearbeitete Zeit: 11. Dezember 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ECRReplicationServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die Ressourcen, die von ECR Replication verwendet oder verwaltet werden

`ECRReplicationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. Dezember 2020, 22:11 Uhr UTC
- Bearbeitete Zeit: 4. Dezember 2020, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElastiCacheServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht es ElastiCache , AWS Ressourcen in Ihrem Namen zu verwalten, sofern dies für die Verwaltung Ihres Caches erforderlich ist

`ElastiCacheServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Dezember 2017, 17:50 Uhr UTC
- Bearbeitete Zeit: 28. November 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElasticLoadBalancingFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon und eingeschränkten Zugriff auf andere Dienste ElasticLoadBalancing, die für die Bereitstellung von ElasticLoadBalancing Funktionen erforderlich sind.

`ElasticLoadBalancingFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElasticLoadBalancingFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. September 2018, 20:42 UTC
- Bearbeitete Zeit: 29. November 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeVpcPeeringConnections",
        "cognito-idp:DescribeUserPoolClient"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "arc-zonal-shift:*",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElasticLoadBalancingReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon ElasticLoadBalancing und abhängige Dienste

`ElasticLoadBalancingReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElasticLoadBalancingReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. September 2018, 20:17 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 18:15 UTC

- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalActivationsDownloadSoftwareAccess

Beschreibung: Zugriff auf gekaufte Ressourcen und Herunterladen der zugehörigen Software und Kickstart-Dateien

`ElementalActivationsDownloadSoftwareAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElementalActivationsDownloadSoftwareAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. September 2020, 17:26 Uhr UTC
- Bearbeitete Zeit: 8. September 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalActivationsFullAccess

Beschreibung: Vollständiger Zugriff, um die von Elemental Appliances und Software gekauften Ressourcen einzusehen und entsprechende Maßnahmen zu ergreifen

`ElementalActivationsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElementalActivationsFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Juni 2020, 21:00 Uhr UTC
- Bearbeitete Zeit: 4. Juni 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalActivationsGenerateLicenses

Beschreibung: Zugriff auf gekaufte Ressourcen und Generierung von Softwarelizenzen für ausstehende Aktivierungen

`ElementalActivationsGenerateLicenses`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElementalActivationsGenerateLicenses` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. August 2020, 18:28 Uhr UTC
- Zeit bearbeitet: 28. August 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalActivationsReadOnlyAccess

Beschreibung: Schreibgeschützter Zugriff auf die detaillierte Liste der gekauften Vermögenswerte, die dem AWS-Konto Benutzer zugeordnet sind

`ElementalActivationsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElementalActivationsReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. August 2020, 16:51 UTC
- Zeit bearbeitet: 28. August 2020, 16:51 UTC

- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalAppliancesSoftwareFullAccess

Beschreibung: Vollständiger Zugriff, um Angebote und Bestellungen von Elemental Appliances und Software einzusehen und entsprechende Maßnahmen zu ergreifen

`ElementalAppliancesSoftwareFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElementalAppliancesSoftwareFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Juli 2019, 16:28 UTC
- Bearbeitete Zeit: 5. Februar 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalAppliancesSoftwareReadOnlyAccess

Beschreibung: Schreibgeschützter Zugriff, um Angebote und Bestellungen von Elemental Appliances und Software einzusehen

`ElementalAppliancesSoftwareReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElementalAppliancesSoftwareReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2020, 22:31 UTC
- Bearbeitete Zeit: 1. April 2020, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalSupportCenterFullAccess

Beschreibung: Uneingeschränkter Zugriff, um Support-Anfragen und Inhalte zum Produktsupport von Elemental Appliance und Software einzusehen und entsprechende Maßnahmen zu ergreifen

`ElementalSupportCenterFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ElementalSupportCenterFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 25. November 2020, 18:08 Uhr UTC
- Bearbeitete Zeit: 5. Februar 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EMRDescribeClusterPolicyForEMRWAL

Beschreibung: Diese Richtlinie gewährt Nur-Lese-Berechtigungen, die es dem WAL-Service für Amazon EMR ermöglichen, den Status eines Clusters zu finden und zurückzugeben.

`EMRDescribeClusterPolicyForEMRWAL`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. Juni 2023, 23:30 UTC
- Bearbeitete Zeit: 15. Juni 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

FMSServiceRolePolicy

Beschreibung: Zugriffsrichtlinie, die es der Rolle ermöglicht, FM-bezogene Aktionen für FM-verwaltete Ressourcen innerhalb eines Kundenorganisationskontos durchzuführen. AWS

`FMSServiceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 28. März 2018, 23:01 UTC
- Bearbeitete Zeit: 22. April 2024, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v29 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WafGeneral",
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
      "Effect" : "Allow",
```

```
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
    },
    {
      "Sid" : "WafWebaclCreation",
      "Effect" : "Allow",
      "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Sid" : "ElbGeneral",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WafPermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
        "waf-regional:GetPermissionPolicy",
```

```
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Sid" : "CloudfrontGeneral",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigScoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation",
        "config:DeleteEvaluationResults"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Sid" : "ConfigUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:PutConfigurationRecorder",
```

```
        "config:StartConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
    },
    {
      "Sid" : "OrganizationsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ShieldGeneral",
      "Effect" : "Allow",
      "Action" : [
```

```
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2SecurityGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SecurityGroupTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "SecurityGroupTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
      "Sid" : "Ec2Unscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Wafv2General",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "Wafv2WebAclAndRuleGroupMutation",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
```

```
      ]
    },
    {
      "Sid" : "Wafv2PermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid" : "Wafv2WebaclDescribe",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "RouteTableTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SubnetTagManagement",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RouteTableCleanup",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "Ec2DescribeUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateVpcEndpointScoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "CreateVpcEndpointUnscoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VpcEndpointsDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RamMutation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamCreation",
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "RamDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamDescribe",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "NetworkFirewallTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkFirewallGeneral",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:PutResourcePolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallCleanup",
```

```
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LogsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupCleanup",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
```

```
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ResolverRuleGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl"
        }
      }
    },
    {
      "Sid" : "NaclTagManagement",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkAclEntry",
        "ec2:CreateNetworkAclEntry",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateNetworkAcl"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

FSxDeleteServiceLinkedRoleAccess

Beschreibung: Ermöglicht Amazon FSx, seine Service Linked Roles für den Amazon S3 S3-Zugriff zu löschen

`FSxDeleteServiceLinkedRoleAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 28. November 2018, 10:40 Uhr UTC
- Zeit bearbeitet: 28. November 2018, 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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_*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GameLiftGameServerGroupPolicy

Beschreibung: Richtlinie, die es Gamelift ermöglicht, Kundenressourcen GameServerGroups zu verwalten

`GameLiftGameServerGroupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `GameLiftGameServerGroupPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. April 2020, 23:12 UTC
- Bearbeitete Zeit: 13. Mai 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GlobalAcceleratorFullAccess

Beschreibung: Erlauben Sie GlobalAccelerator Benutzern vollen Zugriff auf alle APIs

`GlobalAcceleratorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `GlobalAcceleratorFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 02:44 Uhr UTC
- Zeit bearbeitet: 4. Dezember 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GlobalAcceleratorReadOnlyAccess

Beschreibung: Erlauben Sie GlobalAccelerator Benutzern den Zugriff auf schreibgeschützte APIs

`GlobalAcceleratorReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `GlobalAcceleratorReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 02:41 UTC
- Zeit bearbeitet: 27. November 2018, 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GreengrassOTAUpdateArtifactAccess

Beschreibung: Bietet Lesezugriff auf die Greengrass OTA Update-Artefakte in allen Greengrass-Regionen

`GreengrassOTAUpdateArtifactAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `GreengrassOTAUpdateArtifactAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 29. November 2017, 18:11 Uhr UTC
- Bearbeitete Zeit: 18. Dezember 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GroundTruthSyntheticConsoleFullAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die für die Nutzung aller Funktionen der SageMaker Ground Truth Synthetic Console erforderlich sind.

`GroundTruthSyntheticConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `GroundTruthSyntheticConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. August 2022, 15:58 Uhr UTC
- Bearbeitete Zeit: 25. August 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GroundTruthSyntheticConsoleReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Lesezugriff auf SageMaker Ground Truth Synthetic über die. AWS Management Console

`GroundTruthSyntheticConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `GroundTruthSyntheticConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. August 2022, 15:58 Uhr UTC
- Bearbeitete Zeit: 25. August 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Health_OrganizationsServiceRolePolicy

Beschreibung: AWS Gesundheitsrichtlinie zur Aktivierung der Funktion Organizational View

`Health_OrganizationsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Dezember 2019, 13:28 Uhr UTC
- Bearbeitete Zeit: 6. Februar 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMAccessAdvisorReadOnly

Beschreibung: Diese Richtlinie gewährt Lesezugriff auf alle vom IAM Access Advisor bereitgestellten Zugriffsinformationen, z. B. Informationen über den Dienst, auf den zuletzt zugegriffen wurde.

`IAMAccessAdvisorReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IAMAccessAdvisorReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Juni 2019, 19:33 UTC
- Bearbeitete Zeit: 21. Juni 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMAccessAnalyzerFullAccess

Beschreibung: Bietet vollen Zugriff auf IAM Access Analyzer

`IAMAccessAnalyzerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IAMAccessAnalyzerFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Dezember 2019, 17:12 Uhr UTC
- Bearbeitete Zeit: 2. Dezember 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMAccessAnalyzerReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IAM Access Analyzer-Ressourcen

`IAMAccessAnalyzerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IAMAccessAnalyzerReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Dezember 2019, 17:12 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 02:24 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
```

```
        "access-analyzer:ValidatePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMFullAccess

Beschreibung: Bietet vollen Zugriff auf IAM über die AWS Management Console.

`IAMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IAMFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 21. Juni 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IAM über die AWS Management Console.

`IAMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IAMReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 25. Januar 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMSelfManageServiceSpecificCredentials

Beschreibung: Ermöglicht es einem IAM-Benutzer, seine eigenen dienstspezifischen Anmeldeinformationen zu verwalten.

`IAMSelfManageServiceSpecificCredentials`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IAMSelfManageServiceSpecificCredentials` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. Dezember 2016, 17:25 Uhr UTC
- Bearbeitete Zeit: 22. Dezember 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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}"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMUserChangePassword

Beschreibung: Bietet einem IAM-Benutzer die Möglichkeit, sein eigenes Passwort zu ändern.

`IAMUserChangePassword`dist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IAMUserChangePassword` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2016, 00:25 UTC
- Zeit bearbeitet: 15. November 2016, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMUserSSHKeys

Beschreibung: Bietet IAM-Benutzern die Möglichkeit, ihre eigenen SSH-Schlüssel zu verwalten.

`IAMUserSSHKeys`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IAMUserSSHKeys` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:08 UTC
- Bearbeitete Zeit: 9. Juli 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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}"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IVSFullAccess

Beschreibung: Bietet vollen Zugriff auf den Interactive Video Service (IVS). Enthält auch Berechtigungen für abhängige Dienste, die für den vollständigen Zugriff auf die IVS-Konsole erforderlich sind.

`IVSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `IVSFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Dezember 2023, 21:20 UTC
- Bearbeitete Zeit: 13. Dezember 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IVSReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IVS-APIs mit niedriger Latenz und Echtzeit-Streaming

`IVSReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `IVSReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Dezember 2023, 18:00 Uhr UTC
- Bearbeitete Zeit: 16. Februar 2024, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IVSRecordToS3

Beschreibung: Mit dem Service verknüpfte Rolle zur Ausführung von S3 PutObject zur Aufzeichnung von IVS-Livestreams

`IVSRecordToS3`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Dezember 2020, 00:10 UTC
- Bearbeitete Zeit: 5. Dezember 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

KafkaConnectServiceRolePolicy

Beschreibung: Diese Richtlinie gewährt Kafka Connect die Erlaubnis, AWS Ressourcen in Ihrem Namen zu verwalten.

`KafkaConnectServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 7. September 2021, 13:12 UTC
- Bearbeitete Zeit: 7. September 2021, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

KafkaServiceRolePolicy

Beschreibung: Richtlinie für verknüpfte Rollen mit dem IAM-Dienst für Kafka.

`KafkaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2018, 23:31 UTC
- Bearbeitete Zeit: 28. April 2023, 00:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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_*"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

KeyspacesReplicationServiceRolePolicy

Beschreibung: Von Keyspaces für die regionsübergreifende Datenreplikation benötigte Berechtigungen

`KeyspacesReplicationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Mai 2023, 16:15 UTC
- Bearbeitete Zeit: 2. Mai 2023, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:SelectMultiRegionResource",
        "cassandra:Modify",
        "cassandra:ModifyMultiRegionResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

LakeFormationDataAccessServiceRolePolicy

Beschreibung: Richtlinie zur Gewährung von temporärem Datenzugriff auf Lake Formation Formation-Ressourcen

`LakeFormationDataAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Juni 2019, 20:46 UTC
- Bearbeitete Zeit: 6. Februar 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

LexBotPolicy

Beschreibung: Richtlinie für den AWS Lex Bot-Anwendungsfall

`LexBotPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Februar 2017, 22:18 Uhr UTC
- Zeit bearbeitet: 13. November 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

LexChannelPolicy

Beschreibung: Richtlinie für den AWS Lex Channel-Anwendungsfall

`LexChannelPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 17. Februar 2017, 23:23 Uhr UTC
- Zeit bearbeitet: 17. Februar 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

LightsailExportAccess

Beschreibung: Mit dem AWS Lightsail-Service verknüpfte Rollenrichtlinie, die Berechtigungen zum Exportieren von Ressourcen gewährt

`LightsailExportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 28. September 2018, 16:35 Uhr UTC
- Bearbeitete Zeit: 15. Januar 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MediaConnectGatewayInstanceRolePolicy

Beschreibung: Diese Richtlinie gewährt die Erlaubnis, MediaConnect Gateway-Instances auf einem MediaConnect Gateway zu registrieren.

`MediaConnectGatewayInstanceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `MediaConnectGatewayInstanceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 22. März 2023, 20:43 UTC
- Bearbeitete Zeit: 22. März 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MediaPackageServiceRolePolicy

Beschreibung: Ermöglicht das MediaPackage Veröffentlichen von Protokollen in CloudWatch

`MediaPackageServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. September 2020, 17:45 Uhr UTC
- Bearbeitete Zeit: 18. September 2020, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MemoryDBServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht es MemoryDB, AWS Ressourcen in Ihrem Namen zu verwalten, soweit dies für die Verwaltung Ihrer Ressourcen erforderlich ist.

`MemoryDBServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. August 2021, 22:34 UTC
- Bearbeitete Zeit: 18. August 2021, 23:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonMemoryDBManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MemoryDB"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MigrationHubDMSAccessServiceRolePolicy

Beschreibung: Richtlinie für den Database Migration Service, die Rolle im Kundenkonto zu übernehmen, um Migration Hub anzurufen

`MigrationHubDMSAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juni 2019, 17:50 Uhr UTC
- Bearbeitete Zeit: 7. Oktober 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MigrationHubServiceRolePolicy

Beschreibung: Ermöglicht Migration Hub, den Application Discovery Service in Ihrem Namen aufzurufen

`MigrationHubServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juni 2019, 17:22 Uhr UTC
- Bearbeitete Zeit: 6. August 2020, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MigrationHubSMSAccessServiceRolePolicy

Beschreibung: Richtlinie für den Servermigrationsdienst, die Rolle im Kundenkonto zu übernehmen, um Migration Hub anzurufen

`MigrationHubSMSAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juni 2019, 18:30 Uhr UTC
- Bearbeitete Zeit: 7. Oktober 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MonitronServiceRolePolicy

Beschreibung: Richtlinie für die serviceverknüpfte Rolle von AWS Monitron, die Zugriff auf die erforderlichen Kundenressourcen gewährt.

`MonitronServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Mai 2022, 19:22 UTC
- Bearbeitete Zeit: 2. Mai 2022, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung von Amazon Neptune mithilfe der. AWS Management Console Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos, Berechtigungen zum Erstellen und Bearbeiten von Amazon EC2 EC2-Instances und VPC-Konfigurationen, Berechtigungen zum Anzeigen und Auflisten von Schlüsseln in Amazon KMS sowie vollen Zugriff auf Amazon RDS gewährt. Weitere Informationen finden Sie unter https://aws.amazon.com/neptune/faqs/.

`NeptuneConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `NeptuneConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Juni 2018, 21:35 UTC
- Bearbeitete Zeit: 30. November 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Neptune. Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos sowie vollen Zugriff auf Amazon RDS gewährt. Weitere Informationen finden Sie unter https://aws.amazon.com/neptune/faqs/.

`NeptuneFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `NeptuneFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2018, 19:17 UTC
- Bearbeitete Zeit: 22. Januar 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneGraphReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Amazon Neptune Analytics-Ressourcen zusammen mit Leseberechtigungen für abhängige Dienste.

`NeptuneGraphReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `NeptuneGraphReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2023, 07:32 UTC
- Bearbeitete Zeit: 30. November 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon Neptune. Beachten Sie, dass diese Richtlinie auch Zugriff auf Amazon RDS-Ressourcen gewährt. Weitere Informationen finden Sie unter https://aws.amazon.com/neptune/faqs/.

`NeptuneReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `NeptuneReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2018, 19:16 UTC
- Bearbeitete Zeit: 22. Januar 2024, 16:33 UTC

- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NetworkAdministrator

Beschreibung: Gewährt vollständige Zugriffsberechtigungen für AWS Dienste und Aktionen, die für die Einrichtung und Konfiguration von AWS Netzwerkressourcen erforderlich sind.

`NetworkAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `NetworkAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:31 Uhr UTC
- Bearbeitete Zeit: 16. September 2021, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
```

```
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
```

```
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeIpv6Pools",
        "ec2:DetachInternetGateway",
```

```
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:*",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "route53:*",
        "route53domains:*",
        "sns:CreateTopic",
```

```
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLocalGatewayRoute",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteLocalGatewayRoute",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
```

```
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:SearchLocalGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/flow-logs-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
```

```
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ExportTransitGatewayRoutes",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

OAMFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch Observability Access Manager

`OAMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `OAMFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 13:38 UTC
- Zeit bearbeitet: 27. November 2022, 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

OAMReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch Observability Access Manager

`OAMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `OAMReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 13:29 UTC
- Zeit bearbeitet: 27. November 2022, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

OpensearchIngestionSelfManagedVpcePolicy

Beschreibung: Ermöglicht Amazon OpenSearch Ingestion, Netzwerkressourcen zu beschreiben und Servicemetriken in Cloudwatch zu schreiben

`OpensearchIngestionSelfManagedVpcePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Juni 2024, 19:59 UTC
- Bearbeitete Zeit: 10. Juni 2024, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

PartnerCentralAccountManagementUserRoleAssociation

Beschreibung: Ermöglicht den Zugriff auf das Zuordnen und Trennen von Partnern Central-Benutzern zu IAM-Rollen

`PartnerCentralAccountManagementUserRoleAssociation`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `PartnerCentralAccountManagementUserRoleAssociation` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2023, 02:03 UTC
- Bearbeitete Zeit: 10. November 2023, 02:03 UTC

- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

PowerUserAccess

Beschreibung: Bietet vollen Zugriff auf AWS Dienste und Ressourcen, ermöglicht jedoch keine Verwaltung von Benutzern und Gruppen.

`PowerUserAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `PowerUserAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 6. Juli 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeOrganization",
        "account:ListRegions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

QBusinessServiceRolePolicy

Beschreibung: Erteilt Berechtigungen für AWS-Services und Ressourcen, die von Amazon Q verwendet oder verwaltet werden

`QBusinessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. April 2024, 16:05 UTC
- Bearbeitete Zeit: 29. April 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Beschreibung: Richtlinie, die vom QuickSight Team für den Zugriff auf Kundendaten verwendet wird, die von S3 Storage Management Analytics erstellt wurden.

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `QuickSightAccessForS3StorageManagementAnalyticsReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. Juni 2017, 18:18 Uhr UTC
- Bearbeitete Zeit: 8. Oktober 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

RDSCloudHsmAuthorizationRole

Beschreibung: Standardrichtlinie für die Amazon RDS-Servicerolle.

`RDSCloudHsmAuthorizationRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `RDSCloudHsmAuthorizationRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 26. September 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Dienste und Ressourcen.

`ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 16. Mai 2024, 21:10 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v113 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:GetGeneratedPolicy",
        "access-analyzer:ListAccessPreviewFindings",
        "access-analyzer:ListAccessPreviews",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListPolicyGenerations",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
```

```
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetAccountSettings",
        "aoss:GetPoliciesStats",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "appconfig:GetApplication",
        "appconfig:GetConfiguration",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListHostedConfigurationVersions",
```

```
        "appconfig:ListTagsForResource",
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorEntity",
        "appflow:DescribeConnectorFields",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeConnectors",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:DescribeFlows",
        "appflow:ListConnectorEntities",
        "appflow:ListConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "application-autoscaling:ListTagsForResource",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListServicesForAutoScalingConfiguration",
```

```
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:Get*",
        "appsync:List*",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeWorkspace",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetDefaultScraperConfiguration",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
        "aps:ListAlerts",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:QueryMetrics",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "athena:Batch*",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetAssessmentReportUrl",
```

```
        "auditmanager:GetChangeLogs",
        "auditmanager:GetControl",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
        "auditmanager:GetOrganizationAdminAccount",
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "autoscaling-plans:Describe*",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "aws-portal:View*",
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:GetVirtualMachine",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
```

```
        "bedrock:GetDataSource",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListProvisionedModelThroughputs",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
        "braket:GetDevice",
```

```
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "budgets:Describe*",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:ListCostCategoryDefinitions",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
        "chatbot:Describe*",
        "chatbot:Get*",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams",
        "chatbot:ListMicrosoftTeamsUserIdentities",
        "chime:Get*",
        "chime:List*",
```

```
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:GetAudienceGenerationJob",
        "cleanrooms-ml:GetAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModelPolicy",
        "cleanrooms-ml:ListAudienceExportJobs",
        "cleanrooms-ml:ListAudienceGenerationJobs",
        "cleanrooms-ml:ListAudienceModels",
        "cleanrooms-ml:ListConfiguredAudienceModels",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms-ml:ListTagsForResource",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
```

```
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListRepositoriesInDomain",
        "codeartifact:ListTagsForResource",
        "codeartifact:ReadFromRepository",
        "codebuild:BatchGet*",
```

```
        "codebuild:DescribeCodeCoverages",
        "codebuild:DescribeTestCases",
        "codebuild:List*",
        "codecatalyst:GetBillingAuthorization",
        "codecatalyst:GetConnection",
        "codecatalyst:GetPendingConnection",
        "codecatalyst:ListConnections",
        "codecatalyst:ListIamRolesForConnection",
        "codecatalyst:ListTagsForResource",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:List*",
        "codedeploy:BatchGet*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetRepositorySyncStatus",
        "codestar-connections:GetResourceSyncStatus",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListRepositorySyncDefinitions",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar-notifications:ListTargets",
        "codestar:Describe*",
        "codestar:Get*",
```

```
        "codestar:List*",
        "codestar:Verify*",
        "cognito-identity:Describe*",
        "cognito-identity:GetCredentialsForIdentity",
        "cognito-identity:GetIdentityPoolAnalytics",
        "cognito-identity:GetIdentityPoolDailyAnalytics",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetIdentityProviderDailyAnalytics",
        "cognito-identity:GetOpenIdToken",
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:List*",
        "cognito-identity:Lookup*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:Describe*",
        "cognito-idp:Get*",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "cognito-sync:QueryRecords",
        "comprehend:BatchDetect*",
        "comprehend:Classify*",
        "comprehend:Contains*",
        "comprehend:Describe*",
        "comprehend:Detect*",
        "comprehend:List*",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetRecommendationSummaries",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
```

```
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:Describe*",
        "connect:GetContactAttributes",
        "connect:GetCurrentMetricData",
        "connect:GetCurrentUserData",
        "connect:GetFederationToken",
        "connect:GetMetricData",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
        "connect:GetTrafficDistribution",
        "connect:List*",
        "consoleapp:GetDeviceIdentity",
        "consoleapp:ListDeviceIdentities",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
```

```
        "databrew:ListTagsForResource",
        "dataexchange:Get*",
        "dataexchange:List*",
        "datapipeline:Describe*",
        "datapipeline:EvaluateExpression",
        "datapipeline:Get*",
        "datapipeline:List*",
        "datapipeline:QueryObjects",
        "datapipeline:Validate*",
        "datasync:Describe*",
        "datasync:List*",
        "dax:BatchGetItem",
        "dax:Describe*",
        "dax:GetItem",
        "dax:ListTags",
        "dax:Query",
        "dax:Scan",
        "deadline:BatchGetJobEntity",
        "deadline:GetApplicationVersion",
        "deadline:GetBudget",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetWorker",
        "deadline:ListAvailableMeteredProducts",
        "deadline:ListBudgets",
        "deadline:ListFarmMembers",
        "deadline:ListFarms",
        "deadline:ListFleetMembers",
        "deadline:ListFleets",
        "deadline:ListJobMembers",
        "deadline:ListJobs",
```

```
        "deadline:ListLicenseEndpoints",
        "deadline:ListMeteredProducts",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueMembers",
        "deadline:ListQueues",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTagsForResource",
        "deadline:ListTasks",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
```

```
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
        "dms:Describe*",
        "dms:List*",
        "dms:Test*",
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeLaunchConfigurationTemplates",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceNetworks",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListLaunchActions",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "dynamodb:BatchGet*",
```

```
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ec2messages:Get*",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetAuthorizationToken",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchCheck*",
        "ecr:BatchGet*",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elastic-inference:DescribeAcceleratorOfferings",
        "elastic-inference:DescribeAccelerators",
        "elastic-inference:DescribeAcceleratorTypes",
        "elastic-inference:ListTagsForResource",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:Request*",
        "elasticbeanstalk:Retrieve*",
        "elasticbeanstalk:Validate*",
```

```
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:List*",
        "elasticmapreduce:View*",
        "elastictranscoder:List*",
        "elastictranscoder:Read*",
        "elemental-appliances-software:Get*",
        "elemental-appliances-software:List*",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "es:Describe*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "es:Get*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "events:Test*",
        "evidently:GetExperiment",
        "evidently:GetExperimentResults",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegmentReferences",
        "evidently:ListSegments",
```

```
        "evidently:ListTagsForResource",
        "evidently:TestSegmentPattern",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetAction",
        "fis:GetExperiment",
        "fis:GetExperimentTargetAccountConfiguration",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:GetTargetResourceType",
        "fis:ListActions",
        "fis:ListExperimentResolvedTargets",
        "fis:ListExperiments",
        "fis:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "fms:GetAppsList",
        "fms:GetComplianceDetail",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetProtectionStatus",
        "fms:GetProtocolsList",
        "fms:GetViolationDetails",
        "fms:ListAppsLists",
        "fms:ListComplianceStatus",
        "fms:ListMemberAccounts",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "fms:ListTagsForResource",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeExplainability",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribeMonitor",
        "forecast:DescribePredictor",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:DescribeWhatIfAnalysis",
```

```
        "forecast:DescribeWhatIfForecast",
        "forecast:DescribeWhatIfForecastExport",
        "forecast:GetAccuracyMetrics",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListExplainabilities",
        "forecast:ListExplainabilityExports",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListMonitorEvaluations",
        "forecast:ListMonitors",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "forecast:ListWhatIfAnalyses",
        "forecast:ListWhatIfForecastExports",
        "forecast:ListWhatIfForecasts",
        "forecast:QueryForecast",
        "forecast:QueryWhatIfForecast",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetBatchImportJobs",
        "frauddetector:GetBatchPredictionJobs",
        "frauddetector:GetDeleteEventsByEventTypeStatus",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEvent",
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModels",
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
```

```
        "freertos:List*",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
        "gamelift:List*",
        "gamelift:ResolveAlias",
        "gamelift:Search*",
        "glacier:Describe*",
        "glacier:Get*",
        "glacier:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetCrawlers",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetTriggers",
        "glue:BatchGetWorkflows",
        "glue:CheckSchemaVersionValidity",
        "glue:GetCatalogImportStatus",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMapping",
        "glue:GetMLTaskRun",
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
```

```
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetPlan",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:GetWorkflowRunProperties",
        "glue:GetWorkflowRuns",
        "glue:ListCrawlers",
        "glue:ListCrawls",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemas",
        "glue:ListSchemaVersions",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "glue:QuerySchemaVersionMetadata",
        "glue:SearchTables",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListPermissions",
        "grafana:ListTagsForResource",
        "grafana:ListVersions",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
```

```
        "greengrass:Get*",
        "greengrass:List*",
        "groundstation:DescribeContact",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMinuteUsage",
        "groundstation:GetMissionProfile",
        "groundstation:GetSatellite",
        "groundstation:ListConfigs",
        "groundstation:ListContacts",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListGroundStations",
        "groundstation:ListMissionProfiles",
        "groundstation:ListSatellites",
        "groundstation:ListTagsForResource",
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:GetCapabilities",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListFHIRExportJobs",
        "healthlake:ListFHIRImportJobs",
        "healthlake:ListTagsForResource",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "iam:Generate*",
        "iam:Get*",
        "iam:List*",
        "iam:Simulate*",
        "identity-sync:GetSyncProfile",
        "identity-sync:GetSyncTarget",
        "identity-sync:ListSyncFilters",
        "identitystore-auth:BatchGetSession",
        "identitystore-auth:ListSessions",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
```

```
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "importexport:Get*",
        "importexport:List*",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCisScans",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
```

```
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
        "iot1click:ListTagsForResource",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModels",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectors",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetLoggingOptions",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetRegisterAccountStatus",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:GetVehicleStatus",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
```

```
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotroborunner:GetDestination",
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListWorkers",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMetrics",
        "iotwireless:GetMetricConfiguration",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
```

```
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
        "iotwireless:ListQueuedMessages",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStreams",
        "ivs:ListStreamKeys",
        "ivs:ListStreamSessions",
```

```
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:Describe*",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:Get*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafka:ListClusterOperations",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurationRevisions",
        "kafka:ListConfigurations",
        "kafka:ListKafkaVersions",
        "kafka:ListNodes",
        "kafka:ListTagsForResource",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:BatchGetDocumentStatus",
        "kendra:DescribeDataSource",
        "kendra:DescribeExperience",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:DescribePrincipalMapping",
        "kendra:DescribeQuerySuggestionsBlockList",
        "kendra:DescribeQuerySuggestionsConfig",
        "kendra:DescribeThesaurus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots",
        "kendra:ListDataSources",
        "kendra:ListDataSourceSyncJobs",
        "kendra:ListEntityPersonas",
```

```
        "kendra:ListExperienceEntities",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListGroupsOlderThanOrderingId",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListTagsForResource",
        "kendra:ListThesauri",
        "kendra:Query",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Discover*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetEffectivePermissionsForPath",
        "lakeformation:GetLfTag",
        "lakeformation:GetResourceLfTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLfTags",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListTableStorageOptimizers",
        "lakeformation:SearchDatabasesByLfTags",
        "lakeformation:SearchTablesByLfTags",
        "lambda:Get*",
        "lambda:List*",
        "launchwizard:DescribeAdditionalNode",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:DescribeProvisioningEvents",
        "launchwizard:DescribeSettingsSet",
        "launchwizard:GetDeployment",
        "launchwizard:GetInfrastructureSuggestion",
        "launchwizard:GetIpAddress",
```

```
        "launchwizard:GetResourceCostEstimate",
        "launchwizard:GetResourceRecommendation",
        "launchwizard:GetSettingsSet",
        "launchwizard:GetWorkload",
        "launchwizard:GetWorkloadAsset",
        "launchwizard:GetWorkloadAssets",
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:Get*",
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "license-manager:Get*",
        "license-manager:List*",
        "lightsail:GetActiveNames",
```

```
        "lightsail:GetAlarms",
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
        "lightsail:GetBucketAccessKeys",
        "lightsail:GetBucketBundles",
        "lightsail:GetBucketMetricData",
        "lightsail:GetBuckets",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContainerAPIMetadata",
        "lightsail:GetContainerImages",
        "lightsail:GetContainerServiceDeployments",
        "lightsail:GetContainerServiceMetricData",
        "lightsail:GetContainerServicePowers",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperation",
        "lightsail:GetOperations",
        "lightsail:GetOperationsForResource",
        "lightsail:GetRegions",
```

```
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseBlueprints",
        "lightsail:GetRelationalDatabaseBundles",
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAnomalies",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "logs:StartLiveTail",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutequipment:DescribeDataIngestionJob",
        "lookoutequipment:DescribeDataset",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:DescribeLabel",
        "lookoutequipment:DescribeLabelGroup",
        "lookoutequipment:DescribeModel",
        "lookoutequipment:DescribeModelVersion",
        "lookoutequipment:DescribeResourcePolicy",
        "lookoutequipment:DescribeRetrainingScheduler",
        "lookoutequipment:ListDataIngestionJobs",
        "lookoutequipment:ListDatasets",
        "lookoutequipment:ListInferenceEvents",
        "lookoutequipment:ListInferenceExecutions",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutequipment:ListLabelGroups",
        "lookoutequipment:ListLabels",
        "lookoutequipment:ListModels",
```

```
        "lookoutequipment:ListModelVersions",
        "lookoutequipment:ListRetrainingSchedulers",
        "lookoutequipment:ListSensorStatistics",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:Get*",
        "lookoutmetrics:List*",
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "m2:GetApplication",
        "m2:GetApplicationVersion",
        "m2:GetBatchJobExecution",
        "m2:GetDataSetDetails",
        "m2:GetDataSetImportTask",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListApplicationVersions",
        "m2:ListBatchJobDefinitions",
        "m2:ListBatchJobExecutions",
        "m2:ListDataSetImportHistory",
        "m2:ListDataSets",
        "m2:ListDeployments",
        "m2:ListEngineVersions",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:DescribeBuckets",
        "macie2:DescribeClassificationJob",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAdministratorAccount",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetBucketStatistics",
        "macie2:GetClassificationExportConfiguration",
```

```
        "macie2:GetClassificationScope",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetFindingStatistics",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListClassificationJobs",
        "macie2:ListClassificationScopes",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindings",
        "macie2:ListFindingsFilters",
        "macie2:ListInvitations",
        "macie2:ListMembers",
        "macie2:ListOrganizationAdminAccounts",
        "macie2:ListResourceProfileArtifacts",
        "macie2:ListResourceProfileDetections",
        "macie2:ListSensitivityInspectionTemplates",
        "macie2:ListTagsForResource",
        "macie2:SearchResources",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:GetProposal",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNetworks",
        "managedblockchain:ListNodes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListEntitlements",
```

```
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "medialive:DescribeChannel",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannels",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
```

```
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:GetMetricPolicy",
        "mediastore:GetObject",
        "mediastore:ListContainers",
        "mediastore:ListItems",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:ListTags",
        "mgh:Describe*",
        "mgh:GetHomeRegion",
        "mgh:List*",
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:GetReplicationConfiguration",
        "mgn:ListApplications",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListWaves",
        "mobileanalytics:Get*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "monitron:GetProject",
        "monitron:GetProjectAdminUser",
        "monitron:ListProjects",
        "monitron:ListTagsForResource",
```

```
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnections",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkChangeEvents",
        "networkmanager:GetCoreNetworkChangeSet",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetNetworkResourceCounts",
        "networkmanager:GetNetworkResourceRelationships",
        "networkmanager:GetNetworkResources",
        "networkmanager:GetNetworkRoutes",
        "networkmanager:GetNetworkTelemetry",
        "networkmanager:GetResourcePolicy",
        "networkmanager:GetRouteAnalysis",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
```

```
            "networkmanager:ListCoreNetworks",
            "networkmanager:ListPeerings",
            "networkmanager:ListTagsForResource",
            "nimble:GetEula",
            "nimble:GetFeatureMap",
            "nimble:GetLaunchProfile",
            "nimble:GetLaunchProfileDetails",
            "nimble:GetLaunchProfileInitialization",
            "nimble:GetLaunchProfileMember",
            "nimble:GetStreamingImage",
            "nimble:GetStreamingSession",
            "nimble:GetStudio",
            "nimble:GetStudioComponent",
            "nimble:GetStudioMember",
            "nimble:ListEulaAcceptances",
            "nimble:ListEulas",
            "nimble:ListLaunchProfileMembers",
            "nimble:ListLaunchProfiles",
            "nimble:ListStreamingImages",
            "nimble:ListStreamingSessions",
            "nimble:ListStudioComponents",
            "nimble:ListStudioMembers",
            "nimble:ListStudios",
            "nimble:ListTagsForResource",
            "notifications-contacts:GetEmailContact",
            "notifications-contacts:ListEmailContacts",
            "notifications-contacts:ListTagsForResource",
            "notifications:GetEventRule",
            "notifications:GetNotificationConfiguration",
            "notifications:GetNotificationEvent",
            "notifications:ListChannels",
            "notifications:ListEventRules",
            "notifications:ListNotificationConfigurations",
            "notifications:ListNotificationEvents",
            "notifications:ListNotificationHubs",
            "notifications:ListTagsForResource",
            "oam:GetLink",
            "oam:GetSink",
            "oam:GetSinkPolicy",
            "oam:ListAttachedLinks",
            "oam:ListLinks",
            "oam:ListSinks",
            "omics:Get*",
            "omics:List*",
```

```
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
        "osis:GetPipelineChangeProgress",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "personalize:Describe*",
```

```
        "personalize:Get*",
        "personalize:List*",
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
        "polly:Describe*",
        "polly:Get*",
        "polly:List*",
        "polly:SynthesizeSpeech",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetPriceListFileUrl",
        "pricing:GetProducts",
        "pricing:ListPriceLists",
        "proton:GetDeployment",
        "proton:GetEnvironment",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:ListDeployments",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceInstances",
        "proton:ListServices",
        "proton:ListServiceTemplates",
        "proton:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ViewPurchaseOrders",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
```

```
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift-serverless:GetCustomDomainAssociation",
        "redshift-serverless:GetEndpointAccess",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetRecoveryPoint",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:GetScheduledAction",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetTableRestoreStatus",
        "redshift-serverless:GetUsageLimit",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListCustomDomainAssociations",
        "redshift-serverless:ListEndpointAccess",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListRecoveryPoints",
        "redshift-serverless:ListScheduledActions",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTableRestoreStatus",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListUsageLimits",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:ListRecommendations",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
```

```
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetContentModeration",
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppAssessment",
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
```

```
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
```

```
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "sagemaker-groundtruth-synthetic:GetAccountDetails",
        "sagemaker-groundtruth-synthetic:GetBatch",
        "sagemaker-groundtruth-synthetic:GetProject",
        "sagemaker-groundtruth-synthetic:ListBatchDataTransfers",
        "sagemaker-groundtruth-synthetic:ListBatchSummaries",
        "sagemaker-groundtruth-synthetic:ListProjectDataTransfers",
        "sagemaker-groundtruth-synthetic:ListProjectSummaries",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
```

```
        "schemas:List*",
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "securitylake:GetDataLakeExceptionSubscription",
        "securitylake:GetDataLakeOrganizationConfiguration",
        "securitylake:GetDataLakeSources",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
```

```
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "ses:BatchGetMetricData",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "signer:DescribeSigningJob",
        "signer:GetSigningPlatform",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningJobs",
        "signer:ListSigningPlatforms",
        "signer:ListSigningProfiles",
        "signer:ListTagsForResource",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
        "snowball:List*",
        "sns:Check*",
        "sns:Get*",
        "sns:List*",
        "sqs:Get*",
        "sqs:List*",
        "sqs:Receive*",
        "ssm-contacts:DescribeEngagement",
        "ssm-contacts:DescribePage",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
```

```
            "ssm-contacts:ListContactChannels",
            "ssm-contacts:ListContacts",
            "ssm-contacts:ListEngagements",
            "ssm-contacts:ListPageReceipts",
            "ssm-contacts:ListPagesByContact",
            "ssm-contacts:ListPagesByEngagement",
            "ssm-incidents:GetIncidentRecord",
            "ssm-incidents:GetReplicationSet",
            "ssm-incidents:GetResourcePolicies",
            "ssm-incidents:GetResponsePlan",
            "ssm-incidents:GetTimelineEvent",
            "ssm-incidents:ListIncidentRecords",
            "ssm-incidents:ListRelatedItems",
            "ssm-incidents:ListReplicationSets",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:ListTagsForResource",
            "ssm-incidents:ListTimelineEvents",
            "ssm:Describe*",
            "ssm:Get*",
            "ssm:List*",
            "sso-directory:Describe*",
            "sso-directory:List*",
            "sso-directory:Search*",
            "sso:Describe*",
            "sso:Get*",
            "sso:List*",
            "sso:Search*",
            "states:Describe*",
            "states:GetExecutionHistory",
            "states:List*",
            "states:ValidateStateMachineDefinition",
            "storagegateway:Describe*",
            "storagegateway:List*",
            "sts:GetAccessKeyInfo",
            "sts:GetCallerIdentity",
            "sts:GetSessionToken",
            "support:DescribeAttachment",
            "support:DescribeCases",
            "support:DescribeCommunications",
            "support:DescribeServices",
            "support:DescribeSeverityLevels",
            "support:DescribeTrustedAdvisorCheckRefreshStatuses",
            "support:DescribeTrustedAdvisorCheckResult",
            "support:DescribeTrustedAdvisorChecks",
```

```
        "support:DescribeTrustedAdvisorCheckSummaries",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "sustainability:GetCarbonFootprintSummary",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:DescribeReportCreation",
        "tag:Get*",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "timestream:DescribeBatchLoadTask",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListBatchLoadTasks",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "tnb:GetSolFunctionInstance",
        "tnb:GetSolFunctionPackage",
        "tnb:GetSolFunctionPackageContent",
        "tnb:GetSolFunctionPackageDescriptor",
        "tnb:GetSolNetworkInstance",
        "tnb:GetSolNetworkOperation",
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
```

```
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
        "transfer:TestIdentityProvider",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
```

```
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:ListAnswers",
        "wellarchitected:ListCheckDetails",
        "wellarchitected:ListCheckSummaries",
        "wellarchitected:ListLenses",
        "wellarchitected:ListLensReviewImprovements",
        "wellarchitected:ListLensReviews",
        "wellarchitected:ListLensShares",
        "wellarchitected:ListMilestones",
        "wellarchitected:ListNotifications",
        "wellarchitected:ListProfileNotifications",
        "wellarchitected:ListProfiles",
        "wellarchitected:ListProfileShares",
        "wellarchitected:ListReviewTemplateAnswers",
        "wellarchitected:ListReviewTemplates",
        "wellarchitected:ListShareInvitations",
        "wellarchitected:ListTagsForResource",
        "wellarchitected:ListTemplateShares",
        "wellarchitected:ListWorkloads",
        "wellarchitected:ListWorkloadShares",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
```

```
        "workmail:List*",
        "workmail:Search*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ResourceGroupsandTagEditorFullAccess

Beschreibung: Bietet vollen Zugriff auf Resource Groups und den Tag-Editor.

`ResourceGroupsandTagEditorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ResourceGroupsandTagEditorFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 10. August 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ResourceGroupsandTagEditorReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf die Verwendung von Resource Groups und den Tag-Editor, ermöglicht jedoch keine Bearbeitung von Tags über den Tag-Editor.

`ResourceGroupsandTagEditorReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ResourceGroupsandTagEditorReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 10. August 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ResourceGroupsServiceRolePolicy

Beschreibung: Ermöglicht AWS Resource Groups, die AWS Dienste abzufragen, die Ihre Ressourcen besitzen, um die Gruppe zu behalten up-to-date

`ResourceGroupsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Januar 2023, 16:57 UTC
- Bearbeitete Zeit: 5. Januar 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAAmazonEBSCSIDriverOperatorPolicy

Beschreibung: Ermöglicht dem OpenShift Amazon EBS Container Storage Interface (CSI) Driver Operator, den Amazon EBS CSI-Treiber auf einem Red Hat OpenShift Service on AWS (ROSA) - Cluster zu installieren und zu warten. Der Amazon EBS CSI-Treiber ermöglicht es ROSA-Clustern, den Lebenszyklus von Amazon EBS-Volumes für persistente Volumes zu verwalten.

`ROSAAmazonEBSCSIDriverOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAAmazonEBSCSIDriverOperatorPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 22:36 UTC
- Bearbeitete Zeit: 20. April 2023, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSACloudNetworkConfigOperatorPolicy

Beschreibung: Ermöglicht dem OpenShift Cloud Network Config Controller Operator die Bereitstellung und Verwaltung von Netzwerkressourcen für die Nutzung durch das Red Hat OpenShift Service on AWS (ROSA) Cluster-Netzwerk-Overlay. Der OpenShift Cloud Network Operator stellt im Namen der Netzwerk-Plugins eine Schnittstelle zu AWS APIs her über CustomResourceDefinitions. Der Betreiber verwendet diese Richtlinienberechtigungen, um private IP-Adressen für Amazon EC2 EC2-Instances als Teil des ROSA-Clusters zu verwalten.

`ROSACloudNetworkConfigOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSACloudNetworkConfigOperatorPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 22:34 UTC
- Bearbeitete Zeit: 20. April 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAControlPlaneOperatorPolicy

Beschreibung: Ermöglicht der Red Hat OpenShift Service on AWS (ROSA) -Steuerebene, die Ressourcen des ROSA-Clusters Amazon EC2 und Amazon Route 53 zu verwalten.

`ROSAControlPlaneOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAControlPlaneOperatorPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. April 2023, 23:02 UTC
- Bearbeitete Zeit: 30. Juni 2023, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
```

```
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAImageRegistryOperatorPolicy

Beschreibung: Ermöglicht dem OpenShift Image Registry Operator die Bereitstellung und Verwaltung von Amazon S3 S3-Buckets und Objekten für die Nutzung durch die Cluster-Image-Registry Red Hat OpenShift Service on AWS (ROSA), um die ROSA-Speicheranforderungen zu erfüllen. Der OpenShift Image Registry Operator installiert und verwaltet die interne Registrierung eines Red Hat OpenShift Clusters.

`ROSAImageRegistryOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAImageRegistryOperatorPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. April 2023, 20:13 UTC
- Bearbeitete Zeit: 12. Dezember 2023, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
      ]
```

```
    },
    {
      "Sid" : "AllowSpecificObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAIngressOperatorPolicy

Beschreibung: Ermöglicht dem OpenShift Ingress Operator die Bereitstellung und Verwaltung von Load Balancers und DNS-Konfigurationen (Domain Name System) für Red Hat OpenShift Service on AWS (ROSA) -Cluster. Die Richtlinie ermöglicht den Lesezugriff auf Tag-Werte, die der Operator nach Route 53 53-Ressourcen filtert, um gehostete Zonen zu erkennen.

`ROSAIngressOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAIngressOperatorPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 22:37 UTC
- Bearbeitete Zeit: 20. April 2023, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAInstallerPolicy

Beschreibung: Ermöglicht dem Red Hat OpenShift Service on AWS (ROSA) -Installationsprogramm die Verwaltung von AWS Ressourcen, die die ROSA-Clusterinstallation unterstützen. Dies beinhaltet die Verwaltung von Instanzprofilen für ROSA-Worker-Knoten.

`ROSAInstallerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAInstallerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Juni 2023, 21:00 Uhr UTC
- Bearbeitete Zeit: 24. April 2024, 19:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "PassRoleToEC2",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "GetSecretValue",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ManageRecords",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.hypershift.local",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "Route53Manage",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RunInstancesRestrictedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "RunInstancesRedHatOwnedAMIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstancesRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "ListPoliciesAttachedToRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAKMSProviderPolicy

Beschreibung: Ermöglicht dem integrierten ROSA AWS Encryption Provider die Verwaltung von AWS Key Management Service (KMS) -Schlüsseln zur Unterstützung der etcd-Datenverschlüsselung mit einem vom Kunden bereitgestellten AWS KMS-Schlüssel. Die Richtlinie ermöglicht die Verschlüsselung und Entschlüsselung von Daten mithilfe von KMS-Schlüsseln.

`ROSAKMSProviderPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAKMSProviderPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. April 2023, 20:10 UTC
- Bearbeitete Zeit: 27. April 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAKubeControllerPolicy

Beschreibung: Ermöglicht dem ROSA Kubernetes-Controller die Verwaltung von Amazon EC2-, Elastic Load Balancing- (ELB) - und AWS Key Management Service (KMS) -Ressourcen für einen ROSA-Cluster.

`ROSAKubeControllerPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAKubeControllerPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. April 2023, 20:09 UTC
- Bearbeitete Zeit: 16. Oktober 2023, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAManageSubscription

Beschreibung: Diese Richtlinie stellt die Berechtigungen bereit, die für die Verwaltung des Red Hat OpenShift Service On AWS (ROSA) -Abonnements erforderlich sind.

`ROSAManageSubscription`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAManageSubscription` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. April 2022, 20:58 UTC
- Bearbeitete Zeit: 4. August 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSANodePoolManagementPolicy

Beschreibung: Ermöglicht Red Hat OpenShift Service on AWS (ROSA), Cluster-EC2-Instances als Worker-Knoten zu verwalten, einschließlich der Erlaubnis, Sicherheitsgruppen zu konfigurieren und Instances und Volumes zu kennzeichnen. Diese Richtlinie ermöglicht auch die Verwendung von

EC2-Instances mit Festplattenverschlüsselung, die durch AWS Key Management Service (KMS) - Schlüssel bereitgestellt wird.

`ROSANodePoolManagementPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSANodePoolManagementPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Juni 2023, 20:48 UTC
- Bearbeitete Zeit: 2. Mai 2024, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "TerminateInstances",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRequest",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
```

```
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestricted",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
```

```
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSASRESupportPolicy

Beschreibung: Stellt ROSA Site Reliability Engineering (SRE) die erforderlichen Berechtigungen zur Verfügung, um zunächst AWS Ressourcen im Zusammenhang mit Red Hat OpenShift Service on AWS (ROSA) -Clustern zu beobachten, zu diagnostizieren und zu unterstützen, einschließlich der Möglichkeit, den Status des ROSA-Clusterknotens zu ändern.

`ROSASRESupportPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSASRESupportPolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Juni 2023, 14:36 UTC
- Bearbeitete Zeit: 10. April 2024, 20:51 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAWorkerInstancePolicy

Beschreibung: Ermöglicht Red Hat OpenShift Service auf AWS (ROSA) Worker Nodes in Ihrem Konto den schreibgeschützten Zugriff auf Amazon EC2 EC2-Instances und AWS-Regionen für das Lifecycle Management von Rechenknoten.

`ROSAWorkerInstancePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `ROSAWorkerInstancePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 22:35 UTC
- Bearbeitete Zeit: 20. April 2023, 22:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Route53RecoveryReadinessServiceRolePolicy

Beschreibung: Service Linked Role Policy für Route 53 Recovery Readiness

`Route53RecoveryReadinessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. Juli 2021, 16:06 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Route53ResolverServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die von Route53 Resolver verwendeten oder verwalteten Ressourcen

`Route53ResolverServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. August 2020, 17:47 Uhr UTC
- Bearbeitete Zeit: 12. August 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

S3StorageLensServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die Ressourcen, die von S3 Storage Lens verwendet oder verwaltet werden

`S3StorageLensServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2020, 18:15 Uhr UTC

- Zeit bearbeitet: 18. November 2020, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SecretsManagerReadWrite

Beschreibung: Bietet Lese-/Schreibzugriff auf AWS Secrets Manager über die. AWS Management Console Hinweis: Dies schließt IAM-Aktionen aus. Kombinieren Sie es daher mit IAMFullAccess , wenn eine Rotationskonfiguration erforderlich ist.

`SecretsManagerReadWrite`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `SecretsManagerReadWrite` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. April 2018, 18:05 UTC
- Bearbeitete Zeit: 22. Februar 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SecurityAudit

Beschreibung: Die Vorlage für die Sicherheitsüberprüfung gewährt Zugriff auf lesbare Metadaten zur Sicherheitskonfiguration. Es ist nützlich für Software, die die Konfiguration eines überprüft AWS-Konto.

`SecurityAudit`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `SecurityAudit` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 5. April 2024, 17:32 UTC

- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Version der Richtlinie

Richtlinienversion: v42 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
      "Effect" : "Allow",
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
```

```
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appsync:GetApiCache",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
        "auditmanager:ListControls",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling:Describe*",
        "backup:DescribeGlobalSettings",
        "backup:DescribeRegionSettings",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupVaults",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
```

```
        "batch:DescribeJobDefinitions",
        "bedrock:GetCustomModel",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListTagsForResource",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListTagsForResource",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:GetResourcePolicy",
        "codebuild:ListProjects",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:List*",
```

```
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "cognito-sync:Describe*",
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListApprovedOrigins",
        "connect:ListInstanceAttributes",
        "connect:ListInstanceStorageConfigs",
```

```
        "connect:ListInstances",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListLexBots",
        "connect:ListSecurityKeys",
        "databrew:DescribeDataset",
        "databrew:DescribeProject",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "dataexchange:ListDataSets",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
        "datasync:Describe*",
        "datasync:List*",
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
        "devicefarm:ListProjects",
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
```

```
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeImages",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
```

```
        "eks:ListNodeGroups",
        "eks:ListTagsForResource",
        "eks:ListUpdates",
        "elastic-inference:DescribeAccelerators",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elastictranscoder:ListPipelines",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
```

```
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawlers",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDatabases",
        "glue:GetDevEndpoints",
        "glue:GetJobs",
        "glue:GetResourcePolicy",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTags",
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribePublishingDestination",
        "guardduty:Get*",
        "guardduty:List*",
        "health:DescribeAffectedAccountsForOrganization",
        "health:DescribeAffectedEntities",
        "health:DescribeAffectedEntitiesForOrganization",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEventDetails",
        "health:DescribeEventDetailsForOrganization",
        "health:DescribeEventTypes",
        "health:DescribeEvents",
        "health:DescribeEventsForOrganization",
        "health:DescribeHealthServiceStatusForOrganization",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
```

```
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "iot:Describe*",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:List*",
        "iotanalytics:ListChannels",
        "iotevents:ListInputs",
        "iotfleetwise:ListModelManifests",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListWorkspaces",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
```

```
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeLimits",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:List*",
        "lex:DescribeBot",
        "lex:DescribeResourcePolicy",
        "lex:ListBots",
        "license-manager:List*",
        "lightsail:GetBuckets",
        "lightsail:GetContainerServices",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDisks",
        "lightsail:GetInstances",
```

```
        "lightsail:GetLoadBalancers",
        "logs:Describe*",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "machinelearning:DescribeMLModels",
        "macie2:ListFindings",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:ListContainers",
        "memorydb:DescribeClusters",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "nimble:ListStudios",
        "opsworks-cm:DescribeServers",
```

```
        "opsworks:DescribeStacks",
        "organizations:Describe*",
        "organizations:List*",
        "personalize:DescribeDatasetGroup",
        "personalize:ListDatasetGroups",
        "private-networks:ListNetworks",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessPoint",
```

```
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemaVersions",
        "schemas:ListSchemas",
        "schemas:ListTagsForResource",
        "sdb:DomainMetadata",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:ListSecrets",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "serverlessrepo:GetApplicationPolicy",
        "serverlessrepo:List*",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
```

```
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:ListTagsForResource",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAccountSendingEnabled",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetIdentityDkimAttributes",
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListDedicatedIpPools",
        "ses:ListIdentities",
        "ses:ListIdentityPolicies",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueueTags",
        "sqs:ListQueues",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting",
        "ssm:ListAssociationVersions",
        "ssm:ListAssociations",
```

```
            "ssm:ListCommands",
            "ssm:ListComplianceItems",
            "ssm:ListComplianceSummaries",
            "ssm:ListDocumentMetadataHistory",
            "ssm:ListDocumentVersions",
            "ssm:ListDocuments",
            "ssm:ListInventoryEntries",
            "ssm:ListOpsMetadata",
            "ssm:ListResourceComplianceSummaries",
            "ssm:ListResourceDataSync",
            "ssm:ListTagsForResource",
            "sso:DescribeAccountAssignmentCreationStatus",
            "sso:DescribePermissionSet",
            "sso:DescribePermissionsPolicies",
            "sso:List*",
            "states:DescribeStateMachine",
            "states:ListStateMachines",
            "storagegateway:DescribeBandwidthRateLimit",
            "storagegateway:DescribeCache",
            "storagegateway:DescribeCachediSCSIVolumes",
            "storagegateway:DescribeGatewayInformation",
            "storagegateway:DescribeMaintenanceStartTime",
            "storagegateway:DescribeNFSFileShares",
            "storagegateway:DescribeSnapshotSchedule",
            "storagegateway:DescribeStorediSCSIVolumes",
            "storagegateway:DescribeTapeArchives",
            "storagegateway:DescribeTapeRecoveryPoints",
            "storagegateway:DescribeTapes",
            "storagegateway:DescribeUploadBuffer",
            "storagegateway:DescribeVTLDevices",
            "storagegateway:DescribeWorkingStorage",
            "storagegateway:List*",
            "sts:GetAccessKeyInfo",
            "support:DescribeTrustedAdvisorCheckRefreshStatuses",
            "support:DescribeTrustedAdvisorCheckResult",
            "support:DescribeTrustedAdvisorCheckSummaries",
            "support:DescribeTrustedAdvisorChecks",
            "synthetics:DescribeCanaries",
            "synthetics:DescribeCanariesLastRun",
            "synthetics:DescribeRuntimeVersions",
            "synthetics:GetCanary",
            "synthetics:GetCanaryRuns",
            "synthetics:GetGroup",
            "synthetics:ListAssociatedGroups",
```

```
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "tag:GetTagKeys",
        "transcribe:GetCallAnalyticsCategory",
        "transcribe:GetMedicalVocabulary",
        "transcribe:GetVocabulary",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsCategories",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListLanguageModels",
        "transcribe:ListMedicalTranscriptionJobs",
        "transcribe:ListMedicalVocabularies",
        "transcribe:ListTagsForResource",
        "transcribe:ListTranscriptionJobs",
        "transcribe:ListVocabularies",
        "transcribe:ListVocabularyFilters",
        "transfer:Describe*",
        "transfer:List*",
        "translate:List*",
        "trustedadvisor:Describe*",
        "voiceid:DescribeDomain",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:ListTagsForResource",
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAssistant",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
```

```
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
```

```
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SecurityLakeServiceLinkedRole

Beschreibung: Diese Richtlinie gewährt die Erlaubnis, den Amazon Security Lake-Service in Ihrem Namen zu betreiben

`SecurityLakeServiceLinkedRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2022, 14:03 UTC
- Bearbeitete Zeit: 19. April 2024, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigration_ServiceRole

Beschreibung: Berechtigungen, die es dem AWS Server Migration Service ermöglichen, VMs zu EC2 zu migrieren: Ermöglicht dem Server Migration Service, die migrierten Ressourcen dem EC2-Konto des Kunden zuzuweisen.

`ServerMigration_ServiceRole`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `ServerMigration_ServiceRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. August 2020, 20:41 UTC
- Bearbeitete Zeit: 15. Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*/*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigrationConnector

Beschreibung: Berechtigungen, die es dem AWS Server Migration Connector ermöglichen, VMs zu EC2 zu migrieren. Ermöglicht die Kommunikation mit dem AWS Server Migration Service, Lese-/Schreibzugriff auf S3-Buckets, die mit 'sms-b-' und 'import-to-ec2' beginnen, sowie auf die Buckets, die für das AWS Server Migration Connector-Upgrade, AWS die Server Migration Connector-Registrierung mit und das Hochladen von Metriken verwendet werden. AWS AWS

`ServerMigrationConnector`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `ServerMigrationConnector` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Oktober 2016, 21:45 Uhr UTC
- Bearbeitete Zeit: 24. Oktober 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigrationServiceConsoleFullAccess

Beschreibung: Erforderliche Berechtigungen zur Nutzung aller Funktionen der Server Migration Service Console

`ServerMigrationServiceConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ServerMigrationServiceConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Mai 2020, 17:18 Uhr UTC
- Bearbeitete Zeit: 20. Juli 2020, 22:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigrationServiceLaunchRole

Beschreibung: Berechtigungen, die es dem AWS Server Migration Service ermöglichen, für den Start migrierter Server und Anwendungen relevante AWS Ressourcen AWS-Konto für den Kunden zu erstellen und zu aktualisieren.

`ServerMigrationServiceLaunchRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ServerMigrationServiceLaunchRole` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. November 2018, 19:53 UTC
- Zeit bearbeitet: 15. Oktober 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigrationServiceRoleForInstanceValidation

Beschreibung: Berechtigungen, die es der AWS SMS ermöglichen, das verwendete Datenüberprüfungsskript auszuführen und das Erfolgs-/Fehlschlagen des Skripts an SMS zurückzuschicken

`ServerMigrationServiceRoleForInstanceValidation`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ServerMigrationServiceRoleForInstanceValidation` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. Juli 2020, 22:25 Uhr UTC
- Bearbeitete Zeit: 20. Juli 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServiceQuotasFullAccess

Beschreibung: Bietet vollen Zugriff auf Service Quotas

`ServiceQuotasFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ServiceQuotasFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2019, 15:44 Uhr UTC
- Bearbeitete Zeit: 4. Februar 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServiceQuotasReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Service Quotas

`ServiceQuotasReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ServiceQuotasReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2019, 15:31 UTC
- Bearbeitete Zeit: 21. Dezember 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
```

```
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServices",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServiceQuotasServiceRolePolicy

Beschreibung: Ermöglicht Service Quotas, in Ihrem Namen Supportanfragen zu erstellen

`ServiceQuotasServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. Mai 2019, 20:44 UTC
- Bearbeitete Zeit: 24. Juni 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SimpleWorkflowFullAccess

Beschreibung: Bietet vollen Zugriff auf den Simple Workflow-Konfigurationsdienst.

`SimpleWorkflowFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `SimpleWorkflowFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SplitCostAllocationDataServiceRolePolicy

Beschreibung: Ermöglicht das Abrufen AWS von Unternehmensinformationen, falls zutreffend, und das Sammeln von Telemetriedaten für die Datendienste mit geteilter Kostenzuweisung, für die sich der Kunde entschieden hat.

`SplitCostAllocationDataServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. April 2024, 16:05 UTC
- Bearbeitete Zeit: 16. April 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SupportUser

Beschreibung: Diese Richtlinie gewährt Berechtigungen zur Behebung und Lösung von Problemen in einem AWS-Konto. Diese Richtlinie ermöglicht es dem Benutzer auch, den AWS Support zu kontaktieren, um Fälle zu erstellen und zu verwalten.

`SupportUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `SupportUser` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:21 Uhr UTC
- Bearbeitete Zeit: 25. August 2023, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:AcknowledgeJob",
        "codepipeline:AcknowledgeThirdPartyJob",
```

```
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:PollForJobs",
        "codepipeline:PollForThirdPartyJobs",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipeline",
        "cognito-identity:List*",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:Describe*",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:GetBulkPublishDetails",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:GetIdentityPoolConfiguration",
        "cognito-sync:List*",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetResourceConfigHistory",
        "config:ListDiscoveredResources",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ReportTaskProgress",
        "datapipeline:ReportTaskRunnerHeartbeat",
        "devicefarm:List*",
        "devicefarm:Get*",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:ListConfigurations",
        "dms:Describe*",
        "dms:List*",
        "ds:DescribeDirectories",
        "ds:DescribeSnapshots",
```

```
        "ds:GetDirectoryLimits",
        "ds:GetSnapshotLimits",
        "ds:ListAuthorizedApplications",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:Describe*",
        "ec2:DescribeHosts",
        "ec2:describeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNatGateways",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeTags",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:GetRepositoryPolicy",
        "ecr:BatchCheckLayerAvailability",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticbeanstalk:ValidateConfigurationSettings",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "elastictranscoder:ReadJob",
        "elasticfilesystem:DescribeFileSystems",
        "es:Describe*",
        "es:List*",
        "es:ESHttpGet",
        "es:ESHttpHead",
        "events:DescribeRule",
        "events:List*",
        "events:TestEventPattern",
        "firehose:Describe*",
```

```
        "firehose:List*",
        "gamelift:List*",
        "gamelift:Describe*",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:DescribeJob",
        "glacier:Get*",
        "glacier:List*",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "importexport:GetStatus",
        "importexport:ListJobs",
        "inspector:Describe*",
        "inspector:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:DiscoverInputSchema",
        "kinesisanalytics:GetApplicationState",
        "kinesisanalytics:ListApplications",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:List*",
        "lambda:Get*",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "opsworks:Describe*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "redshift:Describe*",
        "route53:Get*",
        "route53:List*",
        "route53domains:CheckDomainAvailability",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
```

```
        "route53domains:List*",
        "s3:List*",
        "sdb:GetAttributes",
        "sdb:List*",
        "sdb:Select*",
        "servicecatalog:SearchProducts",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ScanProvisionedProducts",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "ssm:List*",
        "ssm:Describe*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "waf:Get*",
        "waf:List*",
        "workdocs:Describe*",
        "workmail:Describe*",
        "workmail:Get*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SystemAdministrator

Beschreibung: Gewährt vollständige Zugriffsberechtigungen, die für Ressourcen erforderlich sind, die für Anwendungs- und Entwicklungsvorgänge erforderlich sind.

`SystemAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `SystemAdministrator` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:23 Uhr UTC
- Bearbeitete Zeit: 24. August 2020, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
        "ec2:Allocate*",
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
```

```
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSpotDatafeedSubscription",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DeregisterImage",
```

```
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVolumeIO",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetConsoleOutput",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetLaunchTemplateData",
        "ec2:GetPasswordData",
        "ec2:Import*",
        "ec2:Modify*",
        "ec2:MonitorInstances",
        "ec2:MoveAddressToVpc",
        "ec2:Purchase*",
        "ec2:RegisterImage",
        "ec2:Release*",
        "ec2:Replace*",
        "ec2:ReportInstanceStatus",
        "ec2:Request*",
        "ec2:Reset*",
        "ec2:RestoreAddressToClassic",
        "ec2:RunScheduledInstances",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnmonitorInstances",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticloadbalancing:*",
        "events:*",
        "iam:GetAccount*",
        "iam:GetContextKeys*",
        "iam:GetCredentialReport",
        "iam:ListAccountAliases",
        "iam:ListGroups",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
```

```
        "iam:ListServerCertificates",
        "iam:Simulate*",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:List*",
        "lambda:PublishVersion",
        "lambda:Update*",
        "logs:*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "route53:*",
        "route53domains:*",
        "ses:*",
        "sns:*",
        "sqs:*",
        "trustedadvisor:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
```

```
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl*",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachVolume",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RebootInstances",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "s3:*",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetAccessKeyLastUsed",
        "iam:GetGroup*",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy*",
        "iam:GetRole*",
        "iam:GetSAMLProvider",
```

```
        "iam:GetSSHPublicKey",
        "iam:GetServerCertificate",
        "iam:GetServiceLastAccessed*",
        "iam:GetUser*",
        "iam:ListAccessKeys",
        "iam:ListAttached*",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles*",
        "iam:ListMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListSSHPublicKeys",
        "iam:ListSigningCertificates",
        "iam:ListUserPolicies",
        "iam:Upload*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/ec2-sysadmin-*",
        "arn:aws:iam::*:role/ecr-sysadmin-*",
        "arn:aws:iam::*:role/lambda-sysadmin-*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

TranslateFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Translate.

`TranslateFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `TranslateFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 23:36 UTC
- Bearbeitete Zeit: 8. Januar 2020, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

TranslateReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Translate.

`TranslateReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `TranslateReadOnly` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 18:22 UTC
- Bearbeitete Zeit: 24. Mai 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ViewOnlyAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen zum Anzeigen von Ressourcen und grundlegenden Metadaten für alle AWS Dienste.

`ViewOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `ViewOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:20 Uhr UTC
- Bearbeitete Zeit: 10. Juni 2024, 20:57 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Version der Richtlinie

Richtlinienversion: v19 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "backup:DescribeBackupJob",
        "backup:DescribeBackupVault",
        "backup:DescribeCopyJob",
        "backup:DescribeFramework",
        "backup:DescribeGlobalSettings",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRegionSettings",
        "backup:DescribeReportJob",
        "backup:DescribeReportPlan",
        "backup:DescribeRestoreJob",
        "backup:GetSupportedResourceTypes",
        "backup:ListBackupJobs",
        "backup:ListBackupPlanTemplates",
        "backup:ListBackupPlanVersions",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListCopyJobs",
        "backup:ListFrameworks",
        "backup:ListLegalHolds",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByLegalHold",
        "backup:ListRecoveryPointsByResource",
        "backup:ListReportJobs",
```

```
        "backup:ListReportPlans",
        "backup:ListRestoreJobs",
        "backup:ListTags",
        "batch:ListJobs",
        "bedrock:ListCustomModels",
        "bedrock:ListTagsForResource",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codebuild:ListBuilds*",
        "codebuild:ListProjects",
        "codecommit:List*",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeploymentInstances",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetOnPremisesInstances",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:ListPipelines",
        "codestar:List*",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:List*",
        "cognito-sync:ListDatasets",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:List*",
        "connect:List*",
        "cost-optimization-hub:GetPreferences",
```

```
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListRecommendations",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetAccountLimits",
        "datapipeline:ListPipelines",
        "dax:DescribeClusters",
        "dax:DescribeDefaultParameters",
        "dax:DescribeEvents",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "devicefarm:List*",
        "directconnect:Describe*",
        "discovery:List*",
        "dms:List*",
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeConversionTasks",
```

```
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHost*",
        "ec2:DescribeIdFormat",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetwork*",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnGateways",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "eks:ListTagsForResource",
        "elastic-inference:DescribeAcceleratorOfferings",
        "elastic-inference:DescribeAcceleratorTypes",
```

```
        "elastic-inference:DescribeAccelerators",
        "elastic-inference:ListTagsForResource",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "emr-serverless:ListApplications",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fsx:DescribeFileSystems",
        "gamelift:List*",
        "glacier:List*",
        "glue:GetTags",
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
        "inspector:List*",
        "iot:List*",
        "kafka:ListClusters",
        "kendra:ListDataSources",
        "kendra:ListTagsForResource",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lambda:List*",
```

```
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBots",
        "lex:GetIntentVersions",
        "lex:GetIntents",
        "lex:GetSlotTypeVersions",
        "lex:GetSlotTypes",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "logs:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetImportJobs",
        "mobiletargeting:GetSegments",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "opsworks-cm:Describe*",
        "opsworks:Describe*",
        "organizations:List*",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites",
        "outposts:ListTagsForResource",
        "polly:Describe*",
        "polly:List*",
```

```
        "profile:ListDomains",
        "profile:ListIntegrations",
        "rds:Describe*",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "redshift:DescribeEvents",
        "redshift:ViewQueriesInConsole",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "route53:Get*",
        "route53:List*",
        "route53domains:List*",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
        "ses:DescribeActiveReceiptRuleSet",
        "ses:List*",
        "ses:ListDedicatedIpPools",
        "shield:List*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags",
        "sqs:ListQueues",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ListStateMachines",
        "storagegateway:ListGateways",
```

```
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "trustedadvisor:Describe*",
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "workdocs:DescribeAvailableDirectories",
        "workdocs:DescribeInstances",
        "workmail:Describe*",
        "workspaces:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Sid" : "APIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
```

```
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

VMImportExportRoleForAWSConnector

Beschreibung: Standardrichtlinie für die VM-Import/Export-Servicerolle für Kunden, die den AWS Connector verwenden. Der VM Import/Export-Dienst übernimmt mit dieser Richtlinie eine Rolle bei der Erfüllung von Migrationsanfragen für virtuelle Maschinen von der virtuellen AWS Connector-Appliance. (Beachten Sie, dass der AWS Connector die verwaltete Richtlinie AWSConnector "" verwendet, um Anfragen im Namen des Kunden an den VM Import/Export Service zu richten.) Bietet die Möglichkeit, AMIs und EBS-Snapshots zu erstellen, EBS-Snapshot-Attribute zu ändern,

„Describe*“ -Aufrufe für EC2-Objekte durchzuführen und aus S3-Buckets zu lesen, die mit '2' beginnen. import-to-ec

`VMImportExportRoleForAWSConnector`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `VMImportExportRoleForAWSConnector` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 03. September 2015, 20:48 UTC
- Bearbeitete Zeit: 3. September 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

VPCLatticeFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon VPC Lattice und Zugriff auf Abhängigkeitsdienste.

`VPCLatticeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `VPCLatticeFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. März 2023, 02:49 UTC

- Bearbeitete Zeit: 30. März 2023, 02:49 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

VPCLatticeReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon VPC Lattice über die und eingeschränkten Zugriff auf AWS Management Console Abhängigkeitsdienste.

`VPCLatticeReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `VPCLatticeReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. März 2023, 02:47 UTC
- Bearbeitete Zeit: 30. März 2023, 02:47 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

VPCLatticeServicesInvokeAccess

Beschreibung: Ermöglicht den Zugriff auf das Aufrufen von Amazon VPC Lattice-Diensten.

`VPCLatticeServicesInvokeAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können Verbindungen `VPCLatticeServicesInvokeAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. März 2023, 02:45 UTC
- Bearbeitete Zeit: 30. März 2023, 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WAFLoggingServiceRolePolicy

Beschreibung: SLR erstellen, um Kundenprotokolle in einen Firehose-Stream zu schreiben

`WAFLoggingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. August 2018, 21:05 Uhr UTC

- Bearbeitete Zeit: 24. August 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WAFRegionalLoggingServiceRolePolicy

Beschreibung: SLR erstellen, um Kundenprotokolle in einen Firehose-Stream zu schreiben

`WAFRegionalLoggingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. August 2018, 18:40 Uhr UTC
- Bearbeitete Zeit: 24. August 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WAFV2LoggingServiceRolePolicy

Beschreibung: Diese Richtlinie erstellt eine serviceverknüpfte Rolle, die es AWS WAF ermöglicht, Protokolle in Amazon Kinesis Data Firehose zu schreiben.

`WAFV2LoggingServiceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. November 2019, 00:40 UTC
- Bearbeitete Zeit: 03. Juni 2024, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WellArchitectedConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf das AWS Well-Architected Tool über das AWS Management Console

`WellArchitectedConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `WellArchitectedConsoleFullAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2018, 18:19 Uhr UTC
- Zeit bearbeitet: 29. November 2018, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WellArchitectedConsoleReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf das AWS Well-Architected Tool über AWS Management Console

`WellArchitectedConsoleReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können Verbindungen `WellArchitectedConsoleReadOnlyAccess` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2018, 18:21 Uhr UTC
- Bearbeitete Zeit: 29. Juni 2023, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WorkLinkServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon verwendet oder verwaltet werden WorkLink

`WorkLinkServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können Verbindungen `WorkLinkServiceRolePolicy` zu Ihren Benutzern, Gruppen und Rollen herstellen.

Einzelheiten zu den Richtlinien

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Januar 2019, 19:03 UTC
- Bearbeitete Zeit: 23. Januar 2019, 19:03 UTC

- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "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-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.